


Premier Reference Source

Strategic IT Governance and Performance Frameworks in Large Organizations



EBSCO Publishing : eBook Collection
(EBSCOhost) - printed on 2/8/2023 9:10 PM via
AN: 1988033 ; Maleh, Yassine, Sahid,
Abdelkehir, Belaissaoui, Mustapha. Strategic
IT Governance and Performance Frameworks in
Large Organizations
Account: ns335141



Strategic IT Governance and Performance Frameworks in Large Organizations

Yassine Maleh
The National Port Agency, Morocco

Abdelkebir Sahid
Hassan 1st University, Morocco

Mustapha Belaissaoui
Hassan 1st University, Morocco

A volume in the Advances in
Business Information Systems and
Analytics (ABISA) Book Series



Published in the United States of America by
IGI Global
Business Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: <http://www.igi-global.com>

Copyright © 2019 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher.

Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Names: Maleh, Yassine, 1987- author. | Sahid, Abdelkebir, 1983- author. | Bellaissaoui, Mustapha, 1968- editor.

Title: Strategic IT governance and performance frameworks in large organizations / by Yassine Maleh, Abdelkebir Sahid, and Mustapha Bellaissaoui.

Description: Hershey, PA : Business Science Reference, [2019]

Identifiers: LCCN 2018036395 | ISBN 9781522578260 (hardcover) | ISBN 9781522578277 (ebook)

Subjects: LCSH: Information technology--Management.

Classification: LCC HD30.2 .M3545 2019 | DDC 004.068--dc23 LC record available at <https://lccn.loc.gov/2018036395>

This book is published in the IGI Global book series *Advances in Business Information Systems and Analytics (ABISA)* (ISSN: 2327-3275; eISSN: 2327-3283)

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material.

The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.



Advances in Business Information Systems and Analytics (ABISA) Book Series

ISSN:2327-3275
EISSN:2327-3283

Editor-in-Chief: Madjid Tavana, La Salle University, USA

MISSION

The successful development and management of information systems and business analytics is crucial to the success of an organization. New technological developments and methods for data analysis have allowed organizations to not only improve their processes and allow for greater productivity, but have also provided businesses with a venue through which to cut costs, plan for the future, and maintain competitive advantage in the information age.

The **Advances in Business Information Systems and Analytics (ABISA) Book Series** aims to present diverse and timely research in the development, deployment, and management of business information systems and business analytics for continued organizational development and improved business value.

COVERAGE

- Business Intelligence
- Information Logistics
- Algorithms
- Data Management
- Management Information Systems
- Data Governance
- Business Systems Engineering
- Legal information systems
- Decision Support Systems
- Business Models

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at Acquisitions@igi-global.com or visit: <http://www.igi-global.com/publish/>.

The Advances in Business Information Systems and Analytics (ABISA) Book Series (ISSN 2327-3275) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit <http://www.igi-global.com/book-series/advances-business-information-systems-analytics/37155>. Postmaster: Send all address changes to above address. ©© 2019 IGI Global. All rights, including translation in other languages reserved by the publisher. No part of this series may be reproduced or used in any form or by any means – graphics, electronic, or mechanical, including photocopying, recording, taping, or information and retrieval systems – without written permission from the publisher, except for non commercial, educational use, including classroom teaching purposes. The views expressed in this series are those of the authors, but not necessarily of IGI Global.

Titles in this Series

For a list of additional titles in this series, please visit:

<https://www.igi-global.com/book-series/advances-business-information-systems-analytics/37155>

Sentiment Analysis and Knowledge Discovery in Contemporary Business

Dharmendra Singh Rajput (VIT University, India) Ramjeevan Singh Thakur (Maulana Azad National Institute of Technology, India) and S. Muzamil Basha (VIT University, India)
Business Science Reference • ©2019 • 333pp • H/C (ISBN: 9781522549994) • US \$215.00

Law, Ethics, and Integrity in the Sports Industry

Konstantinos Margaritis (University of Crete, Greece)
Business Science Reference • ©2019 • 307pp • H/C (ISBN: 9781522553878) • US \$195.00

Institutional and Organizational Transformations in the Robotic Era Emerging Research ...

Albena Antonova (Sofia University, Bulgaria)
Business Science Reference • ©2019 • 178pp • H/C (ISBN: 9781522562702) • US \$155.00

Utilizing Big Data Paradigms for Business Intelligence

Jérôme Darmont (Université Lumière Lyon 2, France) and Sabine Loudcher (Université Lumière Lyon 2, France)
Business Science Reference • ©2019 • 313pp • H/C (ISBN: 9781522549635) • US \$210.00

Handbook of Research on Expanding Business Opportunities With Information Systems ...

George Leal Jamil (Informações em Rede Consultoria e Treinamento Ltda, Brazil)
Business Science Reference • ©2019 • 455pp • H/C (ISBN: 9781522562252) • US \$245.00

Qualitative Techniques for Workplace Data Analysis

Manish Gupta (IFHE University, India) Musarrat Shaheen (IFHE University, India) and K. Prathap Reddy (IFHE University, India)
Business Science Reference • ©2019 • 317pp • H/C (ISBN: 9781522553663) • US \$215.00

Machine Learning Techniques for Improved Business Analytics

Dileep Kumar G. (Adama Science and Technology University, Ethiopia)
Business Science Reference • ©2019 • 286pp • H/C (ISBN: 9781522535348) • US \$195.00

For an entire list of titles in this series, please visit:

<https://www.igi-global.com/book-series/advances-business-information-systems-analytics/37155>



701 East Chocolate Avenue, Hershey, PA 17033, USA

Tel: 717-533-8845 x100 • Fax: 717-533-8661

E-Mail: cust@igi-global.com • www.igi-global.com

Table of Contents

Preface	vii
Acknowledgment	xv
Introduction	xvi

Section 1

Strategic Information Technology: Frameworks and Models

Chapter 1

From Information Governance to IT Governance: An Overview of Issues and Frameworks for Large Organizations.....	1
---	---

Chapter 2

A Deep Overview of Information Technology Governance Standards	48
--	----

Section 2

Evaluating Information Technology in Large Organizations

Chapter 3

Evaluation of IT Governance in Middle East and North African Large Organizations	92
--	----

Section 3

Information Technology Agility in Large Organizations

Chapter 4

Strategic Agility Frameworks for Information System Governance.....	138
---	-----

Chapter 5

IT Management Agility in Large Organizations: A Case Study	172
--	-----

Chapter 6	
Managing the Cloud for Information System Agility in Organizations.....	230

Section 4

Information Security Governance in Large Organizations

Chapter 7	
Information Security Governance Practices and Commitments in Organizations	280

Chapter 8	
Information Security Governance in Large Organizations: A Maturity Framework	316

Chapter 9	
Information Security Policy in Large Public Organizations: A Case Study Through ISO 27002	349

Conclusion	403
-------------------------	-----

About the Authors	409
--------------------------------	-----

Index	411
--------------------	-----

Preface

BOOK OVERVIEW

In the age of digitization, the world is evolving at a constant pace (Grover & Kohli, 2012). Companies need to respond to changing conditions and often agility is the only guarantee of survival. Globalization means that there is more competition (Benaroch & Chernobai, 2017). The life cycle of products is shorter than ever (Hagmann, 2013). A disruptive technology can change markets overnight (Bruce, 1998; Chen, Tsou, & Huang, 2009). The company faces challenging challenges in maintaining governance and compliance while achieving its business objectives, complying with current regulations, and managing staff and technology (Kaen, 2005; Moynihan & Pandey, 2010; Nicho, 2016). We understand that IT staff must be able to respond quickly to changing business needs while maintaining existing infrastructure. We also know that the management objective so often cited, “Do more with less” is not just a goal, it is a company commitment. Only effective IT governance is capable of harmonizing all IT components to create business value for the organization (Abdelkebir, Maleh, & Belaissaoui, 2017). Specifically, best practices in IT governance are beginning to be adopted and accepted as they provide guidance to promote and achieve effective IT governance (Shi & Silvius, 2011).

This book discusses the strategic information technology governance in large organizations. There are many books discuss the topics about IT governance. However, the main concept of this book is to explore the strategic IT governance through new approaches (IT Governance maturity in large organization, IT Agility, Information system Security). This book contains four sections and nine chapters to explore this topic. This book is able to explore the characteristics of IT governance on large organizations, as well as provides IT staff, managers, and different IT professional’s frameworks and models to implement an efficient strategic IT governance in the organization.

This book provides sufficient background knowledge and theory about the topic. Furthermore, this book also offers six case studies in large organizations stories, to help readers understand the knowledge, theory and practices. Regarding the complex concepts, this book uses tables and figures to explain them, and cites previous studies or books to provide the models. Through tables and figures, the readers can easily understand and establish the right concepts.

This book describes not only many case studies from International viewpoints, but also collects a lot of literature and researches from database. Hence, this book clearly illustrates the issues, problems, and trends related to the topic, as well as promotes the readers' international viewpoints.

SCOPE

The scope of this guide covers IT governance processes of large companies, which closely associate general management, business lines and IT department.

On the other hand, and despite their importance, it does not cover the operational aspects of IT management, such as project development and the recurring production of services, as long as these are placed entirely under the responsibility of the IT Department and therefore less in interaction with the rest of the organization.

These operational aspects are also dealt with, particularly in the “general IT controls” of the audit. Our approach consists in addressing the IT governance issue through 3 main axes:

- IT governance evaluation in large organizations;
- IT service management, with the integration of new concepts (Agility, cloud computing);
- Information security governance in large organizations.

CHALLENGES

Ensuring an efficient information system in a large organization is a real challenge (Beloglazov et al., 2014; Olson & Wu, 2017). Only a good governance can reassure the general management, customers and partners, shareholders and ultimately the public at large (de Haes & van Grembergen, 2009; Joshi et al., 2018).

Preface

The problem is that the IT governance framework is designed to guide organizations in their global strategy, but does not define the practical framework for the engagement in this strategy (Webb, Pollard, & Ridley, 2006; Weill & Woodham, 2002).

To address these concerns, some practice repositories (ITIL, Cobit, ValIT, CMMi) and international standards (ISO 20000 suite, ISO 15408) now include chapters on IT governance.

The proposed referential and best practices designed to guide organizations in their governance strategy. However, does not define the practical framework to implement or to measure the organization engagement in terms of IT governance.

This book will help organizations to assess their capability maturity state and to address the procedural, technical and human aspects of information system governance and management process.

The main goal of this project is to encourage both researchers and practitioners to share and exchange their experiences and recent studies between academia and industry. The overall objectives are:

- To improve the awareness of readers about Information Technology, concepts, agility and security areas.
- To analyze and present the state-of-the-art of the IT governance and related technologies and methodologies.
- To highlight and discuss the recent development and emerging trends in Information Technology.
- To propose new frameworks, practical solutions and technological advances related to IT governance.

OBJECTIVE

The book aims to promote high-quality research by bringing together researchers and practitioners from academia and industry. This book will present the state of the art and the state of the practice of how to address the following unique information system governance challenges facing emerging technologies. This book is ideally designed for policymakers, students, researchers, academicians, and professionals who are looking for current research that are interested in exploring and implementing an efficient Information System Governance strategies and related technologies.

TARGET AUDIENCE

The target audience of this book will be composed of professionals and researchers working in the field of information security and privacy in various disciplines, e.g. library, information and communication sciences, administrative sciences and management, education, adult education, sociology, computer science, and information technology. Moreover, the book will provide insights and support executives concerned with the management of expertise, knowledge, information and organizational development in different types of work communities and environments.

BOOK ORGANIZATION

The book is organized into four sections and nine chapters. A brief description of each of the chapters follows:

“Introduction” provides the background for the book, introduces the research including the problem being addressed, the motivation for the research, and the book contributions.

Section 1: Strategic Information Technology – Frameworks and Models

Chapter 1, “From Information Governance to IT Governance: An Overview of Issues and Frameworks for Large Organizations,” provides a deep overview of current information governance literature across five key focus areas defined by COBIT 5, business strategic alignment, delivery of value, risk management, management and performance management.

Chapter 2, “A Deep Overview of Information Technology Governance Standards,” presents a comprehensive understanding of the current state of IT governance standards and best practices. This state of the art exploits a frame of reference inspired by the four “worlds” framework that was initially introduced to characterize IT engineering problems.

Section 2: Evaluating Information Technology in Large Organizations

Chapter 3, “Evaluation of IT Governance in Middle East and North African Large Organizations,” provides a deeper understanding of IT governance

Preface

frameworks and their adoption, drawing on established information systems theories. A mixed two-stage approach using quantitative and qualitative studies is used to examine the feasibility of developing an IT governance assessment framework based on COBIT.

Section 3: Information Technology Agility in Large Organizations

Chapter 4, “Strategic Agility Frameworks for Information Technology Governance,” presents different frameworks and models have been presented and studied, with the aim of proposing a specific model that encompasses the advantages of different approaches.

Chapter 5, “IT Management Agility in Large Organizations: A Case Study,” proposes a global and practical strategic framework to improve ITSM service management processes with the additions of two drivers IT Agility management based on DevOps, and IT security management based on SecOps.

Chapter 6, “Managing the Cloud for Information Technology Agility in Large Organizations,” proposes a conceptual framework to improve IT agility, through cloud computing. One of the primary motivation of this research is the lack of fieldwork when considering how cloud computing improves the information systems agility.

Section 4: Information Security Governance in Large Organizations

Chapter 7, “Information Security Governance Practices and Commitments in Organizations,” aims to explore the engagement processes and the practices of organizations involved in a strategy of information security governance. The statistical and econometric analysis of data from a survey of 1000 participants (with a participation rate of 83.67%) from large and medium companies belonging to various industries such as Retail/wholesale, banking, services, Telecom, private and governmental organizations.

Chapter 8, “Information Security Governance in Large Organizations: A Maturity Framework,” aims to discuss the information security governance and to address the weaknesses identified in the literature. Based on practices of information security management and governance described in chapter 8, the authors propose a practical maturity framework for the information security governance and management in organizations. The findings will help organizations to assess their capability maturity state and to address the

procedural, technical and human aspects of information security governance and management process.

Chapter 9, “Information Security Policy in Large Public Organizations: A Case Study Through ISO 27002,” aims to guide organizations in their approach to implementing an IT Security policy. The purpose is to present a practical model of IT security policy based on ISO/IEC 27002:2013 through a case study in a large organization.

“Conclusion” provides the background for the book and introduces the research including the problem being addressed, the motivation for the research, and the book contributions.

Yassine Maleh
National Port Agency, Morocco

Abdelkebir Sahid
Hassan 1st University, Morocco

Mustapha Belaissaoui
Hassan 1st University, Morocco

REFERENCES

Abdelkebir, S., Maleh, Y., & Belaissaoui, M. (2017). An Agile Framework for ITS Management In Organizations: A Case Study Based on DevOps. In *Proceedings of the 2Nd International Conference on Computing and Wireless Communication Systems*. New York: ACM. <http://doi.acm.org/10.1145/3167486.3167556>

Beloglazov, A., Banerjee, D., Hartman, A., & Buyya, R. (2014). Improving Productivity in Design and Development of Information Technology (IT) Service Delivery Simulation Models. *Journal of Service Research*, 18(1), 75–89. doi:10.1177/1094670514541002

Benaroch, M., & Chernobai, A. (2017). Operational IT Failures, IT Value Destruction, and Board-Level IT Governance Changes. *Management Information Systems Quarterly*, 41(3), 729–762. doi:10.25300/MISQ/2017/41.3.04

Bruce, K. (1998). Can You Align IT with Business Strategy? *Strategy and Leadership*, 26(5), 16–20. doi:10.1108/eb054620

Preface

Chen, J. S., Tsou, H. T., & Astrid, Y. H. H. (2009). Service Delivery Innovation: Antecedents and Impact on Firm Performance. *Journal of Service Research*, 12(1), 36–55. doi:10.1177/1094670509338619

de Haes, S., & van Grembergen, W. (2009). An Exploratory Study into IT Governance Implementations and Its Impact on Business/IT Alignment. *Information Systems Management*, 26(2), 123–137. doi:10.1080/10580530902794786

Grover, V., & Kohli, R. (2012). Cocreating IT Value: New Capabilities and Metrics for Multifirm Environments. *Management Information Systems Quarterly*, 36(1), 225–232.

Hagmann, J. (2013). Information Governance – beyond the Buzz. *Records Management Journal*, 23(3), 228–240. doi:10.1108/RMJ-04-2013-0008

Joshi, A., Bollen, L., Hassink, H., De Haes, S., & Van Grembergen, W. (2018). Explaining IT Governance Disclosure through the Constructs of IT Governance Maturity and IT Strategic Role. *Information & Management*, 55(3), 368–380. doi:10.1016/j.im.2017.09.003

Kaen, F. R. (2005). Risk Management, Corporate Governance and the Public Corporation BT - Risk Management: Challenge and Opportunity. Berlin: Springer Berlin Heidelberg.

Moynihan, D. P., & Pandey, S. K. (2010). The Big Question for Performance Management: Why Do Managers Use Performance Information? *Journal of Public Administration: Research and Theory*, 20(4), 849–866. doi:10.1093/jopart/muq004

Nicho, M. (2016). Towards a Taxonomy of Challenges in an Integrated IT Governance Framework Implementation Governance Framework Implementation. *Journal of International Technology and Information Management*, 25(2), 1–32.

Olson & Wu. (2017). *Data Envelopment Analysis in Enterprise Risk Management BT - Enterprise Risk Management Models*. Berlin: Springer Berlin Heidelberg. . doi:10.1007/978-3-662-53785-5_8

Shi, N., & Silvius, G. (2011). *Enterprise IT Governance, Business Value and Performance Measurement*. Hershey, PA: IGI Global.

Webb, P., Pollard, C., & Ridley, G. (2006). Attempting to Define IT Governance: Wisdom or Folly? *Proceedings of the Annual Hawaii International Conference on System Sciences*, 8(C), 1–10.

Weill, P., & Woodham, R. (2002). *Don't Just Lead, Govern: Implementing Effective IT Governance*. CISR Working Paper, 17. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=317319

Acknowledgment

We would like to acknowledge all the people who have helped us in the completion of this book. It is a result of a concentrated and coordinated effort of 16 eminent authors who presented their knowledge and the ideas in the area of security and privacy management, techniques, and protocols. Therefore, first of all, we would like to thank them for their work. Without them, this comprehensive overview of security, privacy and trust technologies in modern data management would have never seen the light of day. Next, we would like to mention Prof. Imed Romdhani and Prof. Abdelkrim Haqiq. Their comments were helpful in making this a better book. Finally, we are very thankful to the team of IGI Global for accepting our book proposal and giving us the opportunity to work on this book project. Particularly, we are thankful to Colleen Moore (Editorial Assistant, Acquisitions), Jordan Tepper (Assistant Development Editor, Acquisitions), and Jan Travers (Director of Intellectual Property and Contracts).

Yassine Maleh
The National Port Agency, Morocco

Abdelkebir Sahid
Hassan 1st University, Morocco

Mustapha Belaissaoui
Hassan 1st University, Morocco

Introduction

BOOK TOPIC

The world is rapidly entering the second machine age, “an inflection point in the history of our economies and societies because of digitization” (Brynjolfsson & McAfee, 2014). From the early 2000s, IT governance ITG became integral to corporate governance and some boards began to wonder how they might govern an area of the business they knew so little about (Weill & Ross, 2004). Yet, most boards continued to ignore or delegate technology matters to management, sometimes several layers down the organization structure (Weill & Woodham, 2002).

Due to the lack of IT governance, many organizations have experienced different types of failures, such as unsuccessful project developments and a loss of competitiveness (Benaroch & Chernobai, 2017). However, it has been shown that companies with above-average IT governance have earned at least 20% higher returns on assets than other companies with lower governance (Weill & Ross, 2004).

Implementing the IT governance is not an easy task, once your own definition and role in the organizations are not clear, and the choice of appropriate IT governance mechanisms continues to demand a great effort.

Reflections on IT governance concern the definition of approaches and the search for the right principles to implement. It is a quest to increase performance and reduce costs and risks (Xue, Liang, & Boulton, 2008).

It is undeniable that the subject of “governance” and the expression “IT governance” or “information system governance” benefit from an important fashionable effect (Weill & Woodham, 2002). However, the questions asked are certainly good questions, essential questions for the proper functioning of an information system. Taking advantage of a fashion effect to (re)launch

Introduction

an internal debate is not necessarily a sign of follow-up. By definition, this fashion is not going to last. But it's an opportunity we can take advantage of. Governance is an essential notion for the information system (Duffield, 2014).

The approaches and action plans implemented under the banner of information system governance are very diverse (Heier, Borgman, & Mervyn, 2007). We propose here a syncretic framework of presentation, that is, a relatively coherent combination that nevertheless mixes different doctrines and systems. This gap is addressed in this research book which seeks to identify different practices through case studies in medium and large organizations.

The main objective of this book is to study the impact and role of the implementation of IT governance practices on the business value derived from IT. This research looks at the gaps between business practices in terms of IT governance and best practices. Several surveys and case studies have been conducted in public and private large organizations, with a final aim to provide readers a practical vision of what IT governance really means.

The purpose of this chapter is to provide the background for the book; introduce the research including the problem being addressed, the motivation for the research and the book contributions. The first section of this chapter discusses the background of the book, which defines the problem statement, the book context and the book proposal. The next sections discuss the significance of the research and its contribution to knowledge. The final section of this chapter outlines the structure of this book.

PROBLEM STATEMENT

There are several outstanding issues regarding the ITG, its mechanisms and its environment. First of all, there is no common definition of ITG and this proves that ITG still has much to evolve (Koooper, Maes, & Lindgreen, 2011). Furthermore, in the absence of a formal ITG, individual managers are left to resolve isolated issues as they arise, and these individual actions can often disagree with each other (Weill & Ross, 2005). Weill and Ross (2005) conducted a survey of nearly 300 companies worldwide and suggest that the ITG is a mystery to key decision-makers in most companies. On average, only one in three senior managers know how IT is managed in their companies. In addition, the implementation of the ITG is influenced by external and internal factors (Xue et al., 2008). But the literature, current frameworks and best practices do not reveal a clear and concise identification of these factors (Pereira & da Silva, 2012).

In addition, it is important to understand how and why a company has adopted a specific ITG agreement to advance knowledge about the effectiveness of alternative governance arrangements in supporting IT-based innovation (de Almeida, 2013).

Previous research has examined the influence of various factors: industry (Ahituv, 1989), firm size (Brown & Magill, 1994), firm strategy (Brown & Magill, 1994), and firm structure (Brown & Magill, 1994; Tavakolian, 1989). However, these studies focus on the singular impacts of specific factors and not on how a set of factors has an impact on ITG agreements. In addition, few researchers attempt to describe and provide a full explanation of the mechanisms of ITG (de Almeida, 2013). Moreover, there is no consensus on all existing ITG mechanisms and there are even conflicting definitions (Almeida et al., 2013).

Therefore, determining the right ITG mechanisms is a complex undertaking (Van Grembergen, 2013). It must also be recognized that what works strategically for one company does not necessarily work for another (Patel 2003), even if they work in the same industrial sector (De Haes & Van Grembergen, 2005). This means that different organizations may need a combination of different structures, processes and relational mechanisms. In summary, there is not a single “best” ITG arrangement because the ITG must respond to the unique environments in which it exists and thus a guide that helps organizations with similar characteristics to implement ITG gaps in the field (Alreemy, Chang, Walters, & Wills, 2016). However, it is possible to create a guide on the most relevant mechanisms to be implemented in a specific organizational context.

BOOK CONTEXT

Although there is significant research on the topic of IT governance (Brown, Grant, & Sprott, 2005), the literature search revealed relatively few studies on the topic of IT governance in acute care (Bradley, Pratt, Byrd, Outlay, & Wynn Jr, 2012). What little research exists tends to focus on reporting structures for IT governance in health care (Smaltz, Carpenter, & Saltz, 2007), and there has been little research that attempts to highlight the importance of IT governance in improving IT adoption in acute care (Bradley et al., 2012). In addition, based on the literature review, there appears to be significant research on the value of IT in large organizations delivery (McCullough et al., 2010) and barriers to IT adoption in large organizations (Lin, Lin, & Roan, 2012).

Introduction

But, little research links the importance of IT governance to maximize this value and address the inherent risks these barriers represent (Bradley, Pratt, Byrd, Outlay, & Wynn Jr, 2012). In developing an IT governance control framework for acute care, this research intends to build on and extend existing IT governance frameworks such as COBIT (ISACA, 2012) and Australian and international standards on IT governance (Standards-Australia, 2010). Using these existing frameworks allows research to focus on IT adoption drivers and IT governance controls that are specific to acute health care. It is recognized, however, that adopting an existing standard as the basis for addressing the primary research question limits somewhat the epistemological and ontological objectives of research. For this research, however, the primary research question is to establish a set of IT governance controls that will improve IT adoption in acute care. The use of an internationally accepted set of IT governance principles has allowed this research to focus on the essence of the primary research question, which the established standards do not address.

BOOK PROPOSAL

This book aims to eliminate inconsistencies in the ITG literature and to obtain a set of ITG models and frameworks used by organizations, taking into account several factors that affect organizations. Such models solve real-world problems because they capture and reuse best practice experiences in a specific professional field (Maleh, Zaydi, Sahid, & Ezzati, 2018). In addition, on the basis of several interviews, a minimum baseline of the ITG mechanisms that large organizations implement is provided. As noted earlier, these models and this minimum baseline will not guarantee 100% successful implementation of the ITG in an organization but should be seen as guidance on which ITG mechanisms may be most relevant to implement in a specific organizational context.

This study is not purely theoretical, but a practical way of examining how ITG can be implemented in organizations to enable them to cope with increasing competition in the marketplace. It should be noted that the main motivation for this book was provided by (Van Grembergen & De Haes, 2009) who suggested that other researchers study the implementation of ITG mechanisms in different contexts. The main contributions of this book are not only the nine chapters that we propose to the scientific community. As already mentioned, this book has examined the impact of the organizational mechanisms of the

ITG and the contingency factors of the ITG in the organizations, and in this way, we offer a minimum reference base that will help large organizations in the implementation of the different mechanisms of the ITG.

CONTRIBUTIONS OF THE BOOK

As applied research, this study attempts to help address the strategic gap in IT governance that has been identified as a significant, real, global problem. In highlighting the “know and do” gap underlying this study, we have tried to tackle this problem boldly. Research overcomes a number of challenges in conducting research in new areas of corporate governance and IT governance. The foundations have been laid for industry and scholarly literature in this field to contribute to knowledge. The establishment of this research has highlighted multiple areas in which this book has been added to the body of knowledge and practice.

This research makes the following significant contributions to IT governance in the literature in large organizations:

- The first contribution of this research is the literature review on IT governance in large organizations. It is clear that while there is significant literature on IT governance and its forms, there is a shortage of literature on IT governance and the importance of internal and external factors on IT investment decision making.
- The second contribution is the first pose of a theoretical model to determine the factors of IT adoption that impact the adoption of IT governance within large organizations. This contribution to research is twofold: 1) the proposed model can be further explored to identify other drivers of IT adoption in organizations that are important from an IT governance perspective; and 2) the constructed theoretical model can be further explored to determine the applicability of such a model to IT governance in general, i.e. independent of the sector or industry.
- The third contribution is a set of empirical IT adoption factors that impact organizations. These internal and external factors were first drawn from the literature and confirmed during this study.
- The fourth contribution is the identification of important aspects that define the agile practical framework for ITSM. It was gathered from a theoretical and empirical research study that generated answers to secondary level research questions and feedback from analysis of best

Introduction

practice experience in organizations. This is the first study to present a comprehensive set of IT governance controls specific to acute healthcare.

- The fifth contribution identifies the determinants of cloud computing adoption based on the characteristics of innovation and the technological, organizational and environmental contexts of organizations, and assesses how cloud computing is changing IS agility.
- The last major contribution to research concerns the IS security governance axis, and includes three sub-contributions. The first explored the determinants of organizations' involvement in information security governance and their practices in this area. The second proposed a framework for measuring information security maturity in large organizations. The last sub-contribution examines which controls are commonly used and how they are selected for the implementation of the information security policy within large public organizations in the Middle East and North Africa MENA through ISO 27002.

REFERENCES

Ahituv, N. (1989). Assessing the value of information: Problems and approaches. *ICIS 1989 Proceedings*.

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). *International Journal of Information Management*, 36(6), 907–916. doi:10.1016/j.ijinfomgt.2016.05.017

Benaroch, M., & Chernobai, A. (2017). Operational IT Failures, IT Value Destruction, and Board-Level IT Governance Changes. *Management Information Systems Quarterly*, 41(3), 729–762. doi:10.25300/MISQ/2017/41.3.04

Bradley, R. V., Pratt, R. M., Byrd, T. A., Outlay, C. N., & Wynn, D. E. Jr. (2012). Enterprise architecture, IT effectiveness and the mediating role of IT alignment in US hospitals. *Information Systems Journal*, 22(2), 97–127. doi:10.1111/j.1365-2575.2011.00379.x

Brown, A. E., Grant, G. G., & Sprott, E. (2005). Framing the Frameworks: A Review of It Governance Research. *Communications of the Association for Information Systems*, 15, 696–712.

Brown, C., & Magill, S. (1994). Alignment of the IS Function with the Enterprise: Toward a Model of Antecedents. *Management Information Systems Quarterly*, 18(4), 4. doi:10.2307/249521

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. WW Norton & Company.

de Almeida, R. S. (2013). *Implementing IT Governance* (Master Thesis). University Tecnico of Leboa.

De Haes, S., & Van Grembergen, W. (2005). IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 237b–237b. 10.1109/HICSS.2005.362

Duffield, M. (2014). *Global governance and the new wars: The merging of development and security*. Z. B. Ltd, Ed.

Heier, H., Borgman, H. P., & Mervyn, G. M. (2007). Examining the relationship between IT governance software and business value of IT: Evidence from four case studies. *Proceedings of the 40th Hawaii International Conference on System Sciences*.

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL: Information Systems Audit and Control Association.

Kooper, M. N., Maes, R., & Lindgreen, E. E. O. R. (2011). On the governance of information: Introducing a new concept of governance to support the management of information. *International Journal of Information Management*, 31(3), 195–200. doi:10.1016/j.ijinfomgt.2010.05.009

Maleh, Y., Zaydi, M., Sahid, A., & Ezzati, A. (2018). Building a Maturity Framework for Information Security Governance Through an Empirical Study in Organizations. In Y. Maleh (Ed.), *Security and Privacy Management, Techniques, and Protocols* (pp. 96–127). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-5583-4.ch004

Introduction

Pereira, R., & da Silva, M. M. (2012). Designing a new integrated IT governance and IT management framework based on both scientific and practitioner viewpoint. *International Journal of Enterprise Information Systems*, 8(4), 1–43. doi:10.4018/jeis.2012100101

Tavakolian, H. (1989). Linking the Information Technology Structure with Organizational Competitive Strategy: A Survey. *Management Information Systems Quarterly*, 13(3), 309–317. doi:10.2307/249006

Van Grembergen, W. (2013). Introduction to the Minitrack “IT Governance and its Mechanisms”-HICSS 2013. *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, 9, 4394–4394. 10.1109/HICSS.2007.292

Van Grembergen, W., & De Haes, S. (2009). *Enterprise governance of information technology: achieving strategic alignment and value*. Springer Science & Business Media.

Weill, P., & Ross, J. (2005). A Matrixed Approach to Designing IT Governance. *MIT Sloan Management Review*, 46(2), 26–34. doi:10.1177/0275074007310556

Weill, P., & Ross, J. W. (2004). *How Top Performers Manage IT Decisions Rights for Superior Results*. In *IT Governance* (pp. 1–10). Harvard Business School Press. doi:10.2139srn.664612

Weill, P., & Woodham, R. (2002). *Don't Just Lead, Govern: Implementing Effective IT Governance*. CISR Working Paper, 17. doi:10.2139srn.317319

Xue, Y., Liang, H., & Boulton, W. R. (2008). Information Technology Governance in Information Technology Investment Decision Processes: The Impact of Investment Characteristics, External Environment, and Internal Context 1. *Management Information Systems Quarterly*, 32(1), 67–96. doi:10.2307/25148829

Section 1

Strategic Information Technology: Frameworks and Models

Chapter 1

From Information Governance to IT Governance: An Overview of Issues and Frameworks for Large Organizations

ABSTRACT

Information governance is more established in organizations. While the need to manage information is not new, new challenges have emerged over the past decade and have grown and become more complex with the opportunities offered by emerging technologies. This chapter provides a deep overview of current information governance literature across five key focus areas defined by COBIT 5: business strategic alignment, delivery of value, risk management, management, and performance management. The chapter focuses on synthesizing the current literature on information governance definitions and issues. The purpose of this chapter is to present a detailed overview of research across information governance definitions in the last two decades. The chapter aims to guide future research in each of the focus areas of information governance.

DOI: 10.4018/978-1-5225-7826-0.ch001

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

The development of digital technologies, the modification of company structures, and the upheaval of practices have undermined these objectives in organizations. The digital tsunami, the big content that is overwhelming society is also affecting organizations (Murphy, Lyytinen, & Somers, 2018). Info-obesity and the dissemination of information within the company risk, if nothing is done to weaken it. They have relied on and many still rely on computer tools to solve their information problems, neglecting to define governance policies. Paradoxically, while it cannot be denied that tools are valuable aids, they are also the source of new challenges. Digital technologies have increased the dispersion of information and the proliferation of documents. The development of digital technology and the increasing simplicity of the tools also gave the illusion that information governance had become unnecessary and that everyone could appropriate the skills needed to manage information. As access to information has become more democratic, the role of the information professional as an intermediary has been called into question. Its competences have been diluted, its functions have been redistributed to other poles or delegated to the user himself. However, the problems of controlling information flows do not only concern technology, but their origin is also often organizational or human (Bailey, Minto-Coy, & Thakur, 2017).

The value of information has also evolved. As an organizational factor, information has become an asset that helps companies to become more competitive. Now seen as capital worth considering, it must be managed as an essential resource and developed (Pang, 2014).

On the other hand, mismanagement is a risk factor (von Solms & van Niekerk, 2013). At a time when regulatory and transparency requirements are increasingly stringent, companies must protect themselves against the risk of legal disputes. It also endangers its image with the loss of information or poor dissemination of data. However, the most frequent problem is the loss of time spent searching for information and thus productivity. Information governance is once again becoming a priority for companies (Joshi, Bollen, Hassink, De Haes, & Van Grembergen, 2018). More and more of them are concerned about these issues and are implementing global or “information governance” policies.

When we talk about information governance, we generally think of large companies but not necessarily small structures. While information volumes

are smaller, and players are closer, they are also affected by the information explosion and, unlike large companies, these difficulties are compounded by a lack of resources to deal with them. What is the situation in the associative world? The risks are certainly less important than in a commercial organization, but the issues related to information control and access are also crucial (Bailey et al., 2017).

While the need to manage information is not new, new challenges have emerged over the past decade and have grown and become more complex with the opportunities offered by digital. These include information overload (infobesity), the multiplication of information sources, the fragility of formats and the plurality of media, as well as an increase in legislation relating to information management.

Information governance is becoming increasingly entrenched, although poorly defined. Very few studies have been carried out on the subject and the reflections come essentially from the practice of professionals. However, public administrations are beginning to implement information governance strategies.

This chapter represents an opportunity to reflect on the issues related to information in organizations and to examine closely, without claiming to be exhaustive, the difficulties and challenges they face; the value of information in companies and the interest of organizing it. The main objective of this chapter is to provide a state of the art on information governance and IT governance definitions, issues and frameworks.

The review of information governance IG literature has been organized using the five key components identified by in COBIT. This chapter attempts to examine various definitions from 1998 to 2018 and investigates difference issues. Then, we analyze existing frameworks of information technology governance through conducting a literature review, classified into five different taxonomies: business strategic alignment, delivery of value, risk management, management and performance management. Finally, we discuss the existent IT governance models and frameworks from 1998 to 2017, and we give some future research directions for the five areas of IT governance.

The next section is the Definitions and Concepts Section including the different definitions of information and IT governance. Followed by the section Information Governance Issues. This section is followed by the main section, IT Governance frameworks, including the classified methods, and a research summary of ITG studies from 1998 to 2017. The next section is the Discussion and Future Research Directions Section. Finally, there is the Conclusion Section.

DEFINITIONS AND CONCEPTS

Almost all definitions of information governance start from the professional literature. Therefore, there is feedback from practice but there is (yet) no academic discipline on the subject. Moreover, for good reason, it is difficult to stand back on a material that is being built. It is, therefore, to ask whether this is not simply a fashion or a simple evolution of language legitimate (Siatiras, 2013).

Before discussing the notion of information governance, it is necessary to focus on what is meant by information. This is perhaps where the question of the scope covered by information governance lies.

Historically, it seems that it is the health sector that has begun to address the concept of information governance, starting from issues related to security and privacy management of patients' personal data (Van Grembergen, 2004).

In the USA, the topic of information governance was mostly specific to the health sector until 2005/2008, when this notion gained momentum to become multi-sectoral and strengthen itself with a view to risk management. It is only since 2011 that the global view integrating the world of data has really begun to be taken into account.

In practice, the definition of information governance generally depends on the vision of the organization senior manager, who considers it as a valid business strategy (Siatiras, 2013). However, let us discuss the views of the main actors in this emerging discipline.

The use of the term governance most often applies to the information and communication technology community. IT governance is a discipline of corporate governance on technological information systems and their performance, as well as risk management (Kooper, Maes, & Lindgreen, 2011; Weill & Ross, 2005). However, the information governance concept is closely linked to the need not to lose control over "risky" information. E-discovery is the challenges of today's world are not new to information specialists such as archivists and record managers. Nevertheless, computing and especially information sharing through the Internet has amplified and made these issues more complex and inevitable. The number of systems [technical or human] that create and value information, or conversely, delete it has exploded. The challenge is therefore above all to create bridges between these systems in order to avoid the risk of partial information management, i.e. limited to the development of different, autonomous and independent points of view.

Information governance IG is about how organizations process or process information. It covers personal, patient/service user and employee information, as well as company information such as financial and accounting records. It enables organizations and individuals to ensure that personal information is handled legally, securely, efficiently and effectively to support the best possible care (Ali, Green, & Robb, 2015).

In addition, it enables organizations to establish procedures and processes for their corporate information that effectively locate and retrieve corporate documents where and when it is needed, particularly to respond to information requests and assist in compliance with corporate governance standards. It provides a framework for gathering all the rules, whether legal or simply best practices, that apply to information processing.

What Is Information Governance?

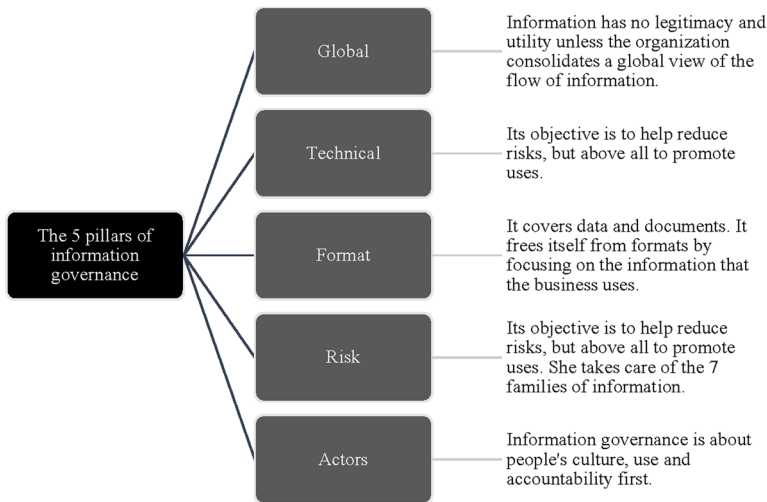
ARMA (Association of records managers and administrators) define information governance as a strategic system composed of standards, processes, roles and metrics that hold natural and legal persons accountable for the production, management and security, in such a way that they respect and contribute to the company's objectives. (Perrein, 2014) identifies five variables around which information governance is structured as shown in Figure 1.

- Strategy and organization before technique.
- The role of technical tools is to facilitate tasks
- A global vision of information flows
- The non-differentiation of formats
- The balance between risk and value

Information governance differs from other issues related to information in organizations, by:

- A systemic, global approach, a desire on the part of organizations to better understand information in the broadest sense. Compared to information management or management, the scope has expanded and is characterized by its transversely. It covers everything to do with information: tools, guidelines, practices, culture, architecture, regulation, business, innovation and above all change. It affects all existing systems: human, organizational, technical, and decision-making.

Figure 1. The 5 pillars of information governance



- A managerial approach. The concept of governance has a strong political connotation. It is part of a management and decision-making dimension. It is based on a governance body whose mission is to lead change and develop new service offerings. Its role is to bring about new behaviors and new uses. It has a role of animation. It is also a question of setting up more consultation, fluidity, participation, transversely and shared responsibilities.

What Is IT Governance?

Despite IT Governance ITG importance and the currency of the term since the late 1990's, academics working in the area continue to define the term in a number of ways (Webb, Pollard, & Ridley, 2006). This lack of a comprehensive definition has possibly impeded in-depth research, further limiting the validity of cross-study comparisons of results (Simonsson, M., & Johnson, 2006). It is thus necessary to clarify the concept of ITG through systematically classifying and drawing together various definitions of ITG in the hope of supporting active research. A variety of definitions of ITG are summarized in Table 1.

These diverse definitions may be classified into three perspectives. Firstly, researchers seek to understand ITG as the location of decision-making rights and accountabilities within organizations. (R Peterson, 2004; Weill

& Woodham, 2002) define ITG as basically decision-making in the IT domain, focusing on the distribution of decision rights and accountabilities (or responsibilities) for the effective use of IT resources.

Secondly, researchers understand ITG as involving the strategic alignment between IT and business in order to achieve enterprises' full business value. (Grembergen, 2004; Webb et al., 2006) define ITG as those activities maximizing business value by bringing about this strategic alignment. In achieving this goal, they emphasize the effective control of resources, performance management, and risk management.

Korac-Kakabadse and Kakabadse (2001) describe IS/ITG as dealing with the structure of relationships and processes aiming to develop, direct and control IS/IT resources such that IT adds value to the firm's pursuit of its strategic objectives. The IT Governance Institute (ITGI, 2003) define ITG as the responsibility of company executives and the board of directors, referring inclusively to the leadership, organizational processes and structures to ensure that the company's IT supports the organization's goals and strategies. ITG concerns IT decision-making, that is, preparation for, making and implementing decisions regarding goals, processes, people and technology on a tactical and strategic level (Simonsson, M., & Johnson, 2006).

In his article, Verhoef (2007) presents an Architecture Theory Diagram ATD, and a framework for defining IT governance based on an extensive literature study. (Ploesser, Recker, & Rosemann, 2008) defines IT Governance is the organizational measurements exercised by the Board, executive management and IT management to control the preparation and implementation of IT strategy. IT governance aims to ensure that the organization and its board of directors or governing body are aware of managing the organization's IT investments responsibly, efficiently and effectively (Bart & Turel, 2010). Scholl, Kubicek, and Cimander (2011) defines the ITG as a set of IT standards, agreements, methodologies, rules and practices that limit, prescribe and enable the implementation and use of ICTs in support of government activity.

In recent works, Aasi, Rusu, and Han (2014) define IT governance as a phase of Preparing, developing and implementing decisions on objectives, processes, people and technology at tactical and strategic levels. Elhasnaoui, Medromi, Chakir, and Sayouti (2015) describe IT governance as the responsibility of the Board of Directors and Executive Management. In her thesis, (Valentine, 2016) confirm that IT governance includes the leadership, alignment and oversight of enterprise technologies with the organization's strategy, structure, systems, policies and governance processes. IT governance seeks to facilitate data-driven decision-making and to minimize risk throughout the enterprise. IT

governance creates value by optimizing stakeholder engagement and strategic investments, and in deriving returns. Felix, Rauschnabel, and Hinsch (2017) propose that the positive effect on performance can be achieved through ITG governance mechanisms that are formally defined, operate with defined rules and standards that are widely disseminated, and are periodically monitored and improved.

Table 1. IT governance definitions

Source	IT Governance Definition
(Rezaee & Reinstein, 1998)	At the conceptual core of IT governance processes is an organizational model of decision making, defined as the process of identifying and solving problems.
(Sambamurthy & Zmud, 1999)	IT-related structures or architectures (and associated authority pattern) implemented to successfully accomplish (IT Imperative) activities in response to an enterprise' environmental and strategic imperatives.
(Korac-Kakabadse & Kakabadse, 2001)	IS/ITG concentrates on the structure of company relationships and processes in seeking to develop, direct and control IS/IT resources. These arrangements add value to organizations as they pursue enterprise goals. ITG aims to balance risk and return for IS/IT resources and their processes.
(Weill & Woodham, 2002)	ITG specifies decision rights and accountability frameworks encouraging the best use within firms of IT.
(ITGI, 2003)	ITG is the responsibility of the board of directors and executive management. It forms an integral part of enterprise governance and consists of the leadership and organizational structures and processes, which ensure that organizations keep and extend their strategy.
(R Peterson, 2004)	ITG describes the distribution of IT decision-making rights and responsibilities among different enterprise stakeholders, defining the procedures and mechanisms for making and monitoring strategic IT decisions.
(Van Grembergen, 2004)	ITG refers to the organizational capacity exercised by the board, executive management and IT management in formulating and implementing IT strategy, as this brings together business and IT.
(Brown, Grant, & Sprott, 2005a)	Specifying the decision rights and accountability frameworks to encourage desirable behavior in using IT.
(Simonsson, M., & Johnson, 2006)	ITG concerns IT decision-making, that is, preparation for, making and implementing decisions regarding goals, processes, people and technology on a tactical and strategic level.
(Webb et al., 2006)	ITG refers to the strategic alignment of IT with business, aiming to release maximum business value through the development and maintenance of effective IT accountability and performance and risk management.
(Verhoef, 2007)	IT governance is a structure of relationships and processes for controlling the IT role in the organization in order to achieve its business goals and add value to the organization.
(Ploesser et al., 2008)	IT Governance is the organizational measurements exercised by the Board, executive management and IT management to control the preparation and implementation of IT strategy.
(Brown, W. A., Laird, R., Gee, C., & Mitra, 2008)	Application of governance to an IT organization and its people, processes and information to guide the way those assets support the needs of the business.
(Van Grembergen, W., & De Haes, 2009)	IT governance is the definition and implementation of processes, structures, and relational mechanisms in the organization that enable both business and IT to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled investments.

continued on following page

From Information Governance to IT Governance

Table 1. Continued

Source	IT Governance Definition
(Bart & Turel, 2010)	IT governance is intended to ensure that the organization and its board of directors or governing body are conscious of managing the organization's IT investment responsibly, efficiently, and effectively.
(Scholl et al., 2011)	Regimes of IT-related standards, agreements, methods, rules, and practices that constrain, prescribe, and enable the implementation and use of ICTs to support government activity.
(Maes, De Haes, & Van Grembergen, 2012)	An integral part of corporate governance [that] addresses the definition and implementation of processes, structures and relational mechanisms in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled investments.
(Grant & Tan, 2013)	A dynamic, goal-directed, performance-driven, adaptive, and relational process that seeks to bring congruence between organizational and IT strategies, structures, systems, processes, and practices in pursuit of valuable, risk-reduced, and measurable returns on IT investment.
(Aasi, P., Rusu, L., & Han, 2014)	Preparation, development and implementation of decisions on goals, processes, people and technology at tactical and strategic levels.
(Elhasnaoui et al., 2015)	IT governance is the responsibility of the Board of Directors and senior management. It is an integral part of corporate governance and includes the leadership and organizational structures and processes that ensure the organization's IT supports and expands the organization's strategy and objectives.
(Valentine, 2016)	Governance of Enterprise Information and Technology supports the board and senior executives in fulfilling their duty of care responsibilities and is an integral part of board governance. IT governance includes the leadership, alignment and oversight of enterprise technologies with the organization's strategy, structure, systems, policies and governance processes.
(Felix et al., 2017)	The positive effect on performance can be achieved through ITG governance mechanisms that are formally defined, operate with defined rules and standards that are widely disseminated, and are periodically monitored and improved.

In short, IT governance can be commonly defined as the clarification of decision-making rights and responsibilities as companies seek to leverage IT assets to business goals. This alignment is designed to allow organizations to achieve their goals by putting in place a systematic series of activities establishing structures and processes. Research suggests that organizations work on three levels in developing IT governance frameworks, designing “structures”, “processes”, and “communication protocols or approaches” (Grembergen, 2004; Weill & Ross, 2004). Structures refer to organizational units and roles responsible for making IT decisions, such as committees, executive teams, and business/IT relationship managers. Processes involve the arrangement of formal decision-making and the design of forms of monitoring checking that daily behavior is consistent with firm IT policy. Monitoring also provides input to decision-making as regards investment proposals and evaluation processes, architecture exception processes, service-level agreements, chargeback, and certain metrics. Communication approaches include announcements, advocates, channels, and education efforts

disseminating IT governance principles and policies. These may also inform workers of the outcomes of IT decision-making processes.

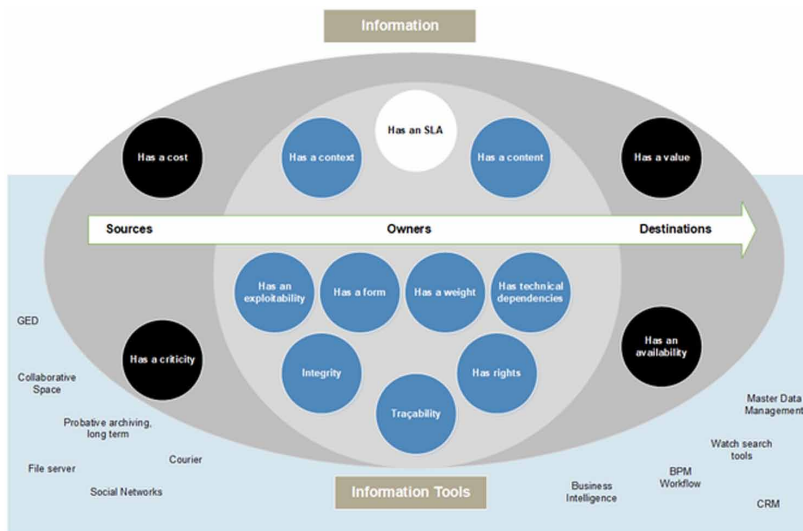
INFORMATION GOVERNANCE ISSUES

The place of information has evolved in the organization. Long considered unproductive, information has become a factor of organization and economic competitiveness. The company must be more responsive and flexible. These new requirements have changed the emphasis on information. The globalization of competition, the rapid evolution of technology, the search for productivity benefits and the shortening of lead times have reinforced the value of knowledge. For (Perrein, 2014), putting information in the context of the company to extract the elements that constitute it. For him, information is:

- **A Form:** Digital, paper
- **A Context:** Its environment, actors, customers, suppliers, products, weather... attached to this information,
- **Technical Dependencies:** Its format requires a particular reader, a particular network (large volume), a particular software...
- **A Weight:** Is it heavy or light information, a film or a transaction amount...
- **A Classification:** Is it categorized and recognized as such structured and clearly defined or without classification,
- **A Content:** The sentence, the sound, the music, the images, the value, the text...
- **A Life Cycle:** An order is transformed into an invoice, a credit request into credit...
- **A Criticality:** To whom can it be communicated, market shares, a salary, a shopping list...
- **Rights:** The information belongs to its creator, its aggregator, its moderator, the end user, the company, can it be modified...
- **A Cost:** Which means are necessary to its creation, its suppression, its operational maintenance?...
- **A Value:** Can it be sold? if it is lost, what financial risk will the company have, a patent, a customer directory, ...”

From Information Governance to IT Governance

Figure 2. Information governance elements

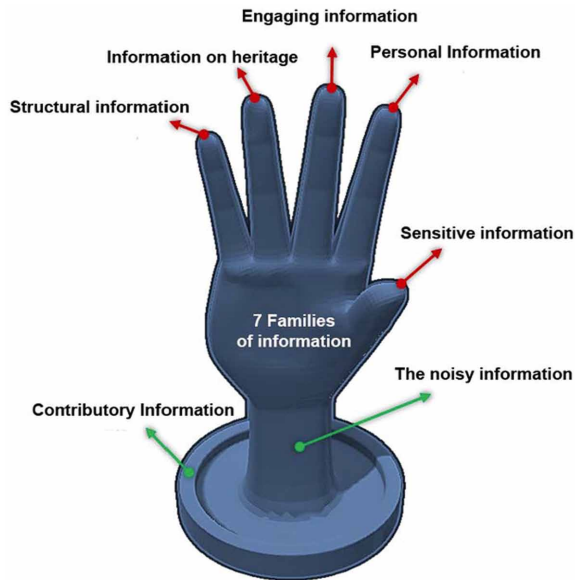


Information Families

Perrein (2014) notes with regret that information governance is most often limited to risk management and regulatory requirements. He categorizes the information in the organizations into 7 families and considers that the first 5 require the definition of a clear policy.

- Binding information, which provides evidence that can be used in the course of a dispute;
- Heritage, represents a value for the organization that must remain accessible over time;
- Structuring, makes it possible to classify the other information, it is formalized by data repositories;
- Sensitive, carrying risks that can put all or part of activities at risk;
- Personal, wears elements that make it possible to identify a natural person or to make him identifiable;
- Contributory carries a certain number of elements making it possible to feed or to constitute the 5 preceding families;
- Noisy has no importance or impact in itself other than to create contributory information.

Figure 3. Information families



Information governance issues are structured along the following areas:

Improving Efficiency

Information Loss

Faced with the loss of information vital to their survival (patents, customer contracts, litigation), companies are anxious to implement effective document management. The inability to reconstitute a complete customer file within a reasonable time, to find the latest version of an electronic document requiring days of work, etc. Although insidious in the digital era, the most frequent crisis is probably loss by dilution.

Ensuring Accessibility

Improving access to information and being able to share it to work more efficiently is the first expectation of companies in terms of information governance. The major and largely dominant challenge is to organize access and sharing information and knowledge. The increase in digital memory and storage capacity, the multiplication of information sources complicate access to the

right information at the right time. While the information activity is supposed to overlap “simply” with the main activity, which remains the production activity, 30% of the managers’ activity is devoted to the information activity (Sauvajol-Riolland, 2010). From 1970 to 1985, scientific reports accessible on the database increased from 52 million to 2 billion. The loss of time in searching for information or documents becomes problematic in companies and is frequently the trigger factor in the search for a structured organization. An International Data Corporation IDC survey of executives revealed some worrying trends regarding lost productivity related to lost time searching for information in the company. This study revealed that these employees spend an average of 7.4 hours per week searching for information without finding it and reformatting data from several sources. The time corresponding to these inefficient practices represents almost \$12,000 per employee per year, calculated on the basis of an average salary (Worthing & Hendriks, 2010).

Protecting Against Risks

Industrial Risk

Ensuring security and safety is a major issue in industries whose activities involve risks. Many disasters are caused by poor documentation. The Bhopal disaster triggered an awareness of the risks associated with poor document management in the industry. In the field of aviation safety, the 2016 (European Aviation Safety Agency) report indicates that documentation anomalies were found by investigators in 25% of incidents, 44% of serious incidents, and 43% of aircraft accidents. Security requirements lead to a large production of documents subject to two major constraints: they must be both able to evolve and be sustainable (EASA, 2016).

Legal Risk

If the case of major disasters is always impressive, the reality will always be the multiplication of disputes and incidents due to obsolete, not up to date, incomplete documentation. The technical document, designed for the maintenance of industrial structures and equipment, changes its role to become a legal document. Depending on the quality in which it has been managed, it may strengthen or weaken a company’s level of protection. Regarding compliance with regulatory requirements, the approach is identical. Companies must

meet increasingly stringent regulatory and normative requirements, as well as transparency requirements for the financial part, which pose the problem of document retention over the long term. Authorities defining regulations and sanctions have multiplied. Companies are increasingly concerned to ensure the traceability of documents in order to demonstrate their compliance. The SerdaLAB study (Jules, 2014) confirms the full development of this issue. Quoted by 4% of respondents in 2011, it obtains 28% of the answers in 2014. Concerns about compliance are also increasing. Regulatory and prescriptive requirements have increased from 14 to 19% in 3 years. Increasing traceability and information security from 28% in 2011 to 37% in 2012, to reach 42% this year [...]”.

Adding Value to Your Capital

Managing knowledge and intangible capital has become an increasingly important concern for the company.

Preserving Knowledge and Expertise

The increase in standardized production has been accompanied by a demand for production knowledge: information on processes, manufacturing methods, technical information produced by the activity... The concept of organizational memory emerged in the United States during the 1990s. Managers realize that expertise and knowledge are resources for the company. The recording of knowledge and a good organization of its dissemination contribute to the company's performance. The company can thus:

- Ensure knowledge transfer
- Achieve productivity benefits.
- Innovating
- Building intangible heritage
- Ensuring knowledge transfer

Ensure Knowledge Transfer

Staff turnover accelerated in the 1980s. The unstable economic context since 1990, the aging of the population accompanied by numerous retirements, waves of redundancies, mergers and takeovers, have caused companies to

lose information and knowledge. Knowledge is not transferred because it is not documented, and its oral transmission is no longer able to take place in this new context. Companies are becoming aware that they are losing information and knowledge that can impact their productivity. The break-up of the company, therefore, requires knowledge to be written and recorded to ensure its transfer to future generations. Extracting knowledge optimizes productivity by helping to reduce research time lost. In some sectors, knowledge maintenance is essential. Failure to record knowledge forces in some situations to repeat what has already been completed.

Achieve Productivity and Quality Benefits

Knowledge is a performance and quality management factor. Knowledge Management enables their capitalization and subsequent reuse. Feedback is used to analyze what has worked and what has not. Knowledge makes it possible to capitalize on an improvement loop and optimize the processes and organization of the workforce. Knowledge gathering allows practices to be readjusted and updated. This presupposes the establishment of repositories as well as a policy and means of sharing.

Innovation

Archiving one's past also avoids constantly reinventing what had already been thought, proposed and realized previously. Innovation is often born of feedback from experience. The company's memorization system becomes a resource center for forecasting or operational staff engaged in immediate action. It allows past experiences to be re-exploited and re-injected into new projects. Sharing experience facilitates training, improving products and services, taking inspiration from a solution to reuse it elsewhere and sometimes giving ideas. Knowledge communication changes knowledge between the parties. Connecting them creates new knowledge. Learning is cumulative. Knowledge creation is more a collective than an individual phenomenon, hence the importance of linking and articulating them. Knowledge is a skill to be shared to change the way things are done.

Building Intangible Heritage

In more than 70% of individual companies or the financial sector, the economic weight of research and development R&D + administration + sales is greater than the capital. Quality has been replaced by the knowledge which becomes a competitive advantage. Innovation makes the value of the product.

In an unstable environment, knowledge is a factor of stability. We have entered an era of the knowledge economy. It is a lever for economic development. The intangible capital of a company is based on the brand, the customer portfolio, and its capacity to innovate... which represents on average 9 times the tangible capital. A company's wealth is calculated according to its human capital, its customer capital and its organizational capital (patents, innovation).

Win as a Decision

Information is a factor in resolving uncertainty. Strategic information is the result of a process of transforming heterogeneous data into information through analysis that precedes decision-making. Centralizing information feeds the company's thinking about itself, as a decision-making and strategic management support body. However, companies often look outside for information that is already available internally but that is little shared or archived. By developing its capital and giving itself the possibilities to exploit it, the company reduces the need to seek information from outside, which leads to time wasted in analyses and verifications.

Drawing on experience and lessons from history also helps decision-making. The company relies on its past to direct its actions. Looking back allows the company to analyze what has contributed to its success or, on the contrary, to look back on its failures. Some companies go so far as to have their history written and use it as a forecasting tool. Conversely, the saturation of information has the effect of degrading the decision-making process.

Save Money

Improved productivity and security contribute to the company's financial benefits. On the other hand, downtime, production recalls in industry, accidents have a high financial cost and a cost in terms of image. The cost of sanctions and procedures is significantly higher than the cost of implementing an

archiving policy. Organizations are increasingly concerned with achieving sustainable development benefits. Reducing printouts, redundancies and copies contributes to this, as does reduce and sharing documentary collections. Saving money by lowering IT storage costs is a growing concern in organizations as well. Storage capacity is increasing at a lower cost. However, volumes are increasing faster than storage costs are falling. At present, few companies perceive the economic benefit and it is clearly not a sufficient reason to launch into information governance, but it is progressing steadily according to the SerdaLAB study. According to a study by Coleman Parkes Research, 77% of companies believe that implementing governance would reduce costs. According to the IDC study, the optimization of customer-oriented document processes improves turnover by an average of 10%.

Maintaining Reputation

Poor information governance impacts the company's image on two levels. Internally, it can induce psycho-social risks. The feeling of never being able to catch up with the flow of information leads managers to discouragement and guilt. Hence a situation of stress and anxiety, generating other dysfunctions for the organization (Sauvajol-Riolland, 2010). Externally, a bad diffusion of confidential documents can harm his image. Companies are looking to improve the security of their information. 76% of organizations faced a serious business and/or compliance risk from inefficient document processes (BLANGER, 2013).

IT GOVERNANCE FRAMEWORKS FOR LARGE ORGANIZATIONS

A comprehensive IG program should include IT governance. IT governance is the primary means by which stakeholders can ensure that IT investments create business value and contribute to the achievement of business objectives. This strategic alignment of IT with business is both challenging and essential. IT governance programs go further and aim to improve IT performance and deliver optimal business value while meeting regulatory compliance requirements (Benaroch & Chernobai, 2017).

While the CIO is generally responsible for the implementation of IT governance, the CEO and Board of Directors must receive reports and updates

to fulfill their IT governance responsibilities and to ensure that the program is working well and delivering business benefits (Turel & Bart, 2014).

In recent decades, board members have generally not been involved in overseeing IT governance. Computer science was a mysterious and frightening art, and they didn't want to dive in and get shot down by a smart-alec technology genius. However, today, it is a critical and inevitable responsibility, and frameworks have been put in place to manage IT efforts.

Several IT governance frameworks can guide the implementation of an IT governance program. Although frameworks and guidelines such as CobiT, ITIL, ValIT and ISO 38500 (Simonsson & Johnson, 2006) have been widely adopted, there is no absolute standard IT governance framework; the combination that works best for an organization depends on business factors, corporate culture, IT maturity and staffing capacity. The level of implementation of these frameworks will also vary by organization.

IT governance is a relatively new term, first coming into general use in the late 1990s (Magnusson, 2010). Until about 2009, definitions of IT governance tended to primarily focus on creating the right settings for the effective internal management of technological infrastructure and IT department (Ali & Green, 2009; Weill & Ross, 2005; Xue, Liang, & Boulton, 2008). IT departments were expected to deal with a multitude of different issues including rapid technological change over a very short time period. "Boards needed little or no understanding of technological issues because the technology was simply a tool to implement a strategy" (Carter & Lorsch, 2004). Thus the role of IT governance originally had an internal and primarily operational focus. From around 2003, however, a growing range of scholars began to consider IT governance as deserving board attention (Cater-Steel, 2009). Perhaps awareness of the need to distinguish between governance and management arose because "new technologies are themselves creating strategic choice for businesses worldwide" (Carter, C. B., & Lorsch, 2004). Others brought the integration of corporate governance and ITG closer, suggesting IT governance involving boards needed to be integral to overall enterprise or corporate governance (Wim Van Grembergen, 2013).

One of the most commonly used definitions, applicable at the board level, describes Enterprise IT Governance (EITG) as an integral part of corporate governance that addresses the definition and implementation of relational processes, structures and mechanisms within the organization. Enabling both companies and IT professionals to fulfill their responsibilities in support of business and IT alignment and business value creation from IT-enabled investments (Wim Van Grembergen, 2013).

Every company or organization is structured around its missions and in order to achieve the objectives it has set itself. Its activity defines its orientations. It gathers and coordinates a set of means to carry them out and defines itself as a system, “that is to say, as a set of interacting elements, grouped within a piloted structure, having a communication system to facilitate the circulation of information, with the aim of responding to needs and achieving specific objectives.

Some researchers have sought to develop a more comprehensive ITG framework by combining a variety of existing definitions and approaches. In general, frameworks designate the structure of a set of objects within a given domain, besides describing the relationships among those objects (Brown, Grant, & Sprott, 2005b). The organizing effect of frameworks is especially useful during the early stages of research in a domain in delineating a research area, providing a foundation for the description of knowledge, and uncovering or highlighting opportunities for more specific theory development and testing within the domain in question (Dibbern, Goles, Hirschheim, & Jayatilaka, 2004).

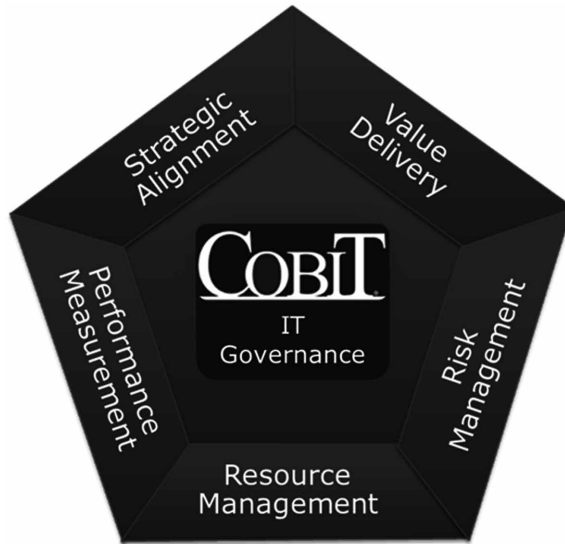
Research Methodology

This section provides a detailed review of research literature over the past two decades on the five key focus areas of ITG. We started by selecting articles published between 1998 and 2017, which represent the state of the art of recent literature on IT governance. To do this, we have selected only papers published in Q1 journals and conferences such as MIS Quarterly, emerald, the International Journal of Accounting Information Systems, or leading conferences such as the Hawaii International Conference on System Sciences.

One of the most frequently referenced frameworks in ITG is the Control Objectives for Information and related Technology (COBIT) framework as proposed by ITGI. ITGI, established in 1998 to advance international thinking and standards in directing and controlling enterprises’ information technology, offers the COBIT framework as a tool for integrating and institutionalizing good practices, ensuring individual enterprises’ IT supports their business objectives.

In the COBIT framework, the IT governance focus area is divided into five subareas as shown in Figure 4: strategic alignment, value delivery, resource management, risk management, and performance management. These five areas consist of topics which executive management needs to address in

Figure 4. COBIT IT governance areas



governing IT within their enterprises (ITGI, 2005). A description of each ITG subareas is shown in Figure 5.

IT Governance Frameworks

Table 2 presents the main IT governance models in literature according to the classification in Figure 5.

Figure 5. IT governance focus areas in COBIT

Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Management
<ul style="list-style-type: none"> • Focuses on ensuring strong connections between business and IT plans, defining, maintaining and validating IT value propositions; and aligning IT with enterprise operations. 	<ul style="list-style-type: none"> • Executes value propositions throughout the delivery cycle, ensuring that IT delivers promised benefits against business strategies, optimizing costs and proving the intrinsic value of IT. 	<ul style="list-style-type: none"> • Specifies the optimal investment in, and the proper management of, critical IT resources, including applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure. 	<ul style="list-style-type: none"> • Defines risk awareness among senior corporate officers, stressing the need to understand enterprises' risk appetite, compliance requirements, and transparency; embeds risk management responsibilities within the organization. 	<ul style="list-style-type: none"> • Tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards translating strategy into action to achieve goals not captured by conventional accounting methods.

Table 2. IT governance frameworks

Theoretical Framework	ITG Focus Area	Empirical/Case Study	Research Summary
(Bruce, 1998)	Strategic alignment	No data	Recognized culture, decision-making processes, customers, investments, organization, performance measures and strategy as keys to operationalizing alignment.
(Luftman, Papp, & Brier, 1999)	Strategic alignment	Executives attending classes at IBM's Advanced Business Institute	Determined the factors on which organizations that have successfully aligned are focused.
(Reich & Benbasat, 2000)	Strategic alignment	10 business units in the Canadian Life Insurance Industry	Examined the influence of several factors on the social dimension of alignment and tested short and long-term alignment aspects within business units.
(Hirschheim & Sabherwal, 2001)	Strategic alignment	Case studies of 3 large Australian organizations	Proposed strategic IS alignment model with four components being a business strategy, IS role, IS sourcing and IS structure.
(GOLD, 2002)	Strategic alignment	No data	The identified link between critical success factors for IS systems and Business strategy.
(Luftman, 2003)	Strategic alignment	Tested on 50 global 2000 companies	Identified 6 IT-business alignment criteria or maturity categories – Communications, competency/value measurement, governance, partnership, technology scope and skills.
(Avison, Jones, Powell, & Wilson, 2004) (2004)	Strategic alignment	Financial services firm in Australia	Tested Strategic Alignment Model (SAM) by applying data from completed projects to determine the usefulness of this model.
(S. De Haes & Van Grembergen, 2005a)	Strategic alignment	Belgian financial organization	Provided guidance for practitioners on the practical application of IT Governance processes and analysis of organizational ITG structures, processes and relational mechanisms provided
(Cumps, Viaene, Dedene, & Vandenbulcke, 2006)	Strategic alignment	Empirical Study in European Organisations	Analyzed business and ICT alignment to derive practical guidelines for managers, and develops an alignment score measure consisting of 6 alignment skill groups.
(Van Lier & Dohmen, 2007)	Strategic alignment	6 organizations	Discussed the links between benefits management and strategic alignment and their influence on IT.
((Dong, Liu, & Yin, 2008)	Strategic alignment	Empirical Study on Chinese Firms	Measured business strategy, information system strategy, and information system strategic alignment built a conceptual model to describe the relationship between these factors and investigated their implications for information system performance and business performance.
(Steven de Haes & van Grembergen, 2009)	Strategic alignment	Case studies of the Belgian financial services sector	Explored how organizations are implementing IT governance and to analyze the relationship between these implementations and business/IT alignment.

continued on following page

Table 2. Continued

Theoretical Framework	ITG Focus Area	Empirical/Case Study	Research Summary
(L. Chen, 2010)	Strategic alignment	Empirical Study on 22 companies in China	The relationship between the maturity dimensions of alignment and the strategic alignment of the IS was then examined. Business alignment maturity in China was assessed to provide a snapshot of business and IT alignment in China.
(Nianxin Wang, Yajiong Xue, Huigang Liang, & Shilun Ge, 2011)	Strategic alignment	case studies with 2 Chinese firms	Revealed Business information technology alignment BITA revolutions and identify their external and internal antecedents.
(Bradley, R. V., Pratt, R. M., Byrd, T. A., Outlay, C. N., & Wynn Jr, 2012)	Strategic alignment	survey data from 164 US hospitals	Enterprise architecture maturity indirectly influences the effectiveness of IT resources when IT alignment is incorporated as a mediating variable.
(Charoensuk, Wongsurawat, & Khang, 2014)	Strategic alignment	Data collected from business and IT personnel from 3 to 5-star hotels in Thailand	Explored that knowledge in the shared domain had the highest relationship with IT alignment and that IT management sophistication had the least impact, but in a negative direction, while the organizational size was a moderator.
(Alaceva & Rusu, 2015)	Strategic alignment	A case study in a large Swedish company	Demonstrated that poor understanding of the counterparty environment, poor communication, unclear specifications, limited cooperation and lack of mutual commitment and support hinders the achievement of alignment between the business and IT domains with the social dimension.
(El-Mekawy, Rusu, & Perjons, 2015)	Strategic alignment	Interviews from large Swedish organizations.	Proposed a framework of 25 criteria divided into four groups. It has been tested on six large BITA models, demonstrating its feasibility. Finally, the framework was evaluated by interviewing five consultants and seven IT managers from large Swedish organizations.
(Renaud, Walsh, & Kalika, 2016)	Strategic alignment	Bibliometric data collected in 2011, and again in 2014	Proposed an explanation for practitioners' apparent failures to fulfill SAM's intended contribution.
(Goni et al., 2017)	Strategic alignment	Case analysis in Malaysian public Higher Education Institutions	Underscored the important role of information systems during the sustainability implementation.
(Menon & Lee, 2000)	Value Delivery	Washington State Department of Health Hospital Database	IT value is assessed by considering overall efficiency, technical efficiency and allocative efficiency
(McKay, Marshall, & Smith, 2003)	Value Delivery	Interviews with CIO of six of Australia's Top 50 companies	Suggested that at the heart of a good IT governance practice is an integrated cycle of business case development, alignment and prioritization, evaluation, systems acquisition and proactive realization of benefits after implementation.

continued on following page

From Information Governance to IT Governance

Table 2. Continued

Theoretical Framework	ITG Focus Area	Empirical/Case Study	Research Summary
(Weill & Ross, 2004)	Value Delivery	250 enterprises across 23 countries	Identified five main factors that relate to variations in governance patterns being strategic and performance goals, organizational structure, governance experience, size and diversity, industry and regional differences
(Gregor, Martin, Fernandez, Stern, & Vitale, 2006)	Value Delivery	1050 organizations of varying sizes from 15 of the 17 Australian and NZ standard industry classification codes	Assessed issues associated with the circumstances and settings of ICT implementation, ICT contribution, factors which influence the value, what management practices relate to ICT benefit.
(Kwon & Watts, 2006)	Value Delivery	A survey IT Managers	Investigated the impact on the firm performance of two types of IT value practices – efficiency and knowledge management and looks at the relationship to dynamism and hostility.
(Heier, H., Borgman, H. P., & Mervyn, 2007)	Value Delivery	4 international implementation sites	Considered the impact of ITG software on value delivery from IT systems, and examines the relationship between ITG applications, ITG processes and value delivery from IT.
(Spohrer & Maglio, 2008)	Value Delivery	No Data	Described the emergence of service science, a new interdisciplinary area of study that aims to address the challenge of becoming more systematic about innovating in service.
(J.-S. Chen, Tsou, & Huang, 2009)	Value Delivery	An empirical study of financial firms in Taiwan	Identified innovation orientation, external partner collaboration, and information technology capability as the antecedents of service delivery innovation and analyze the impact of service delivery innovation on firm performance.
(Nazımoğlu & Özsen, 2010)	Value Delivery	Observations and some interviews with employees IBM Service Delivery	Defined and analyze risks within information technologies (IT) in service delivery. Some specific risks that appear in IT service delivery and the relationships between risks will be defined.
(Hsieh, Rai, & Xu, 2011)	Value Delivery	Multi-source longitudinal data collected through a field study of one of the world's largest telecommunications service providers in China and USA	Exploited the sensorial perception theory to develop a model to understand the history, contingencies and consequences of prolonged use of customer relationship management (CRM) technologies by customer service employees.
(Grover & Kohli, 2012)	Value Delivery	No Data	Highlighted a contemporary issue of cocreating IT value through four layers of relational arrangement between firms that seek to be agile and innovative.
(Beloglazov, Banerjee, Hartman, & Buyya, 2014)	Value Delivery	A proof-of-concept product line of several related IBM's IT service delivery systems	Created a design artifact to build product lines of IT service delivery simulation models, simplifying and significantly reducing the cost of designing and developing simulation models.

continued on following page

Table 2. Continued

Theoretical Framework	ITG Focus Area	Empirical/Case Study	Research Summary
(Tsai, Chou, Leu, Chen, & Tsaur, 2015)	Value Delivery	Survey data listed from TOP 5000 manufacturing and service companies in Taiwan	Provided an effective measure of ERP performance within an ITG framework, and provided evidence of partial mediating effects of value delivery between service quality and ERP performance.
(Vlietland, van Solingen, & van Vliet, 2016)	Value Delivery	A case study in a large multinational financial institute. The case concerns a set of 6 co-dependent Scrum Teams	Supported companies that suffer from such dependencies with a governance framework that helps them mitigate collaboration problems between sets of co-dependent Scrum teams.
(Benaroch & Chernobai, 2017)	Value Delivery	An empirical study in U.S. public financial firms	Proved that after experiencing IT operational failures, companies are making improvements in the level of IT competence of their boards of directors, and the improvements are proportional to the degree of negative market reaction.
(Karimi, J., Bhattacharjee, A., Gupta, Y. P., & Somers, 2000)	Resource Management	213 IT managers in the financial services industry	Examined the impact of IT steering committees on the management of IT functions.
(R. R. Peterson, 2001)	Resource Management	3 Large European Based Financial Services Organizations	Extended the theoretical model proposed by the same author in 2000, and develops 4 research propositions to test the mode.
(Ryan Peterson, Parker, Ribbers, Peterson, & Parker, 2002)	Resource Management	9 Large complex organizations in different industries across Europe and North America	Examined the procedural and social mechanisms of IT governance.
(Schwarz & Hirschheim, 2003)	Resource Management	6 Case Studies in Oil and Gas Industry	Developed a model of IT governance • Explores difference in perceptions toward IT and the organization of IT activities.
(R Peterson, 2004)	Resource Management	Case Study of Johnson & Johnson	Presented a holistic view of IT governance, and considered that structural, process and relational capabilities are all important aspects of effective ITG.
(S. De Haes & Van Grembergen, 2005b)	Resource Management	8 industries Case Studies	Discussed the relationship between business goals, IT goals and IT processes, and gathers preliminary evidence of the relationship
(Mills, Viaene, & Ribbers, 2006)	Resource Management	12 Large ICT projects in Banking and insurance industry	Examined the role of the ICT project evaluation process especially the feasibility evaluation, and establishes a link between the main trigger for a project and the thoroughness of the feasibility process
(Steven De Haes & Van Grembergen, 2006)	Resource Management	Pilot case studies in Belgian Organizations	Developed a research question, which focused on the link between IT governance and fusion between business and IT Extend the prior work of De Haes and Van Grembergen (2004).

continued on following page

Table 2. Continued

Theoretical Framework	ITG Focus Area	Empirical/Case Study	Research Summary
(Chênevert & Tremblay, 2009)	Resource Management	statistical analyses performed on 128 Canadian companies	Reveals that the use of an extensive relational empowerment strategy is significantly and negatively related to voluntary turnover when accompanied by a compensation program that rewards performance.
(Lengnick-Hall, Beck, & Lengnick-Hall, 2011)	Resource Management	No data	Proposed that an organization's resilience capacity be developed through strategic human resources management to create skills among core employees that, when clustered at the organizational level, enable organizations to respond resiliently to severe shocks.
(Maes, K., De Haes, S., & Van Grembergen, 2013)	Resource Management	A case study in a large organization in Belgium	Explored a case study in order to identify multiple business case tasks that complement the process of (Peppard, J., Ward, J., & Daniel, 2007).
(Aasi, P., Rusu, L., & Han, 2014)	Resource Management	Literature review	Identified how culture and IT governance in the companies can be linked together and promote this area for future research.
(Wiedemann, Weeger, & Gewald, 2015)	Resource Management	Multiple case study in large Financial Assurance and Manufacturing organizations	Identified critical success factors for IT service delivery ITSD management.
(Hagen & Bouchard, 2016)	Resource Management	Survey	Identified portions of the literature in the areas of Information Technology (IT) management, skills development, and curriculum development that support the design of a holistic conceptual framework for instruction in non-technical skills within the IT higher education context.
(Altemimi & Zakaria, 2017)	Resource Management	Malaysia Public Sector Case Study	Identified the domain of IT governance and provide insights practice with each domain that was detected through literature.
(Dickinson, 2001)	Risk Management	No data	Enterprise risk management is a systematic and integrated approach to the management of the total risks that a company faces.
(Young & Jordan, 2002)	Risk Management	A case study of project failure	Established the theoretical groundwork to develop an integrated approach to risk management and IT governance.
(Spira & Page, 2003)	Risk Management	Literature review	Explored sociological perspectives on risk and its conceptualization to frame the debate about internal control and risk management within the UK corporate governance arena.
(Kaen, 2005)	Risk Management	No data	Addressed the connection between risk management and corporate governance and the public corporation.
(Gewald & Helbig, 2006)	Risk Management	A case study of a large outsourcing service provider	Developed a governance model for mitigating outsourcing risks. The proposed model consists of strategic direction, governance principles and organizational structures.

continued on following page

Table 2. Continued

Theoretical Framework	ITG Focus Area	Empirical/Case Study	Research Summary
(Wipplinger, 2007)	Risk Management	Several case studies	Provided the most current information needed to understand and implement Value at Risk VAR-as well as manage newer dimensions of financial risk.
(Laeven & Levine, 2009)	Risk Management	Empirical assessment	Showed that the relation between bank risk and capital regulations, deposit insurance policies, and restrictions on bank activities depend critically on each bank's ownership structure, such that the actual sign of the marginal effect of regulation on risk varies with ownership concentration.
(Van Greuning & Brajovic Bratanovic, 2009)	Risk Management	Case studies in the financial sector	Argued that each of the key players in the corporate governance process (such as shareholders, directors, executive managers, and internal and external auditors) is responsible for some component of financial and operational risk management.
(Gillet, Hübner, & Plunus, 2010)	Risk Management	8000 case studies analyzing operational risk loss events	Examined stock market reactions to the reporting of operational losses by financial companies, and distinguished between operational losses and reputational damage. The analysis covers 154 events from the FIRST OpVantage database.
(Hoyt & Liebenberg, 2011)	Risk Management	A detailed search of financial reports, newswires, and other media for evidence of ERM use	Measured the extent to which specific firms have implemented ERM programs and, then, to assess the value implications of these programs, and focused on U.S. insurers in order to control for differences that might arise from regulatory and market differences across industries.
(Aebi, Sabato, & Schmid, 2012)	Risk Management	Sample data of 372 banks	Investigated whether corporate governance mechanisms related to risk management, such as the presence of a Chief Risk Officer (CRO) on a bank's board of directors and whether the CRO reports to the CEO or directly to the board, are associated with improved bank performance during the 2007/2008 financial crisis.
(Ellul, A., & Yerramilli, 2013)	Risk Management	A case study at US bank holding companies (BHCs)	Suggested that a strong and independent risk management function can curtail tail risk exposures at banks.
(Lam, 2014)	Risk Management	Several case studies	Addressed the key concepts, processes, and tools underlying risk management, and lays out clear strategies to manage what is often a highly complex issue.
(Olson, David L. et WU, 2015)	Risk Management	No Data	Highlighted three events directly involving risk management. One was natural, the 2010 BP oil spill in the Gulf of Mexico. The Enron financial fiasco was only one of a number of cases where business fraud adversely impacted the U.S. economy. The 2008 real estate meltdown had an even greater impact.

continued on following page

Table 2. Continued

Theoretical Framework	ITG Focus Area	Empirical/Case Study	Research Summary
(Brustbauer, 2016)	Risk Management	Empirical study	Suggested that SMEs follow an active or passive ERM approach, which affects their strategic orientation; a passive approach leads to a defensive strategy and an active approach, an offensive strategy.
(Hopkinson, 2017)	Risk Management	Several case studies	Described the issues facing anyone tasked with assessing project risk management capability.
Van Grembergen and Van Bruggen (1997)	Performance Management	No data	Developed IT balanced scorecard based on original balanced scorecard approach of (Kaplan, R. S., & Norton, 1992).
(Otley, 1999)	Performance Management	No data	Proposed a framework for analyzing the operation of management control systems structured around five central issues. These issues relate to objectives, strategies and plans for their attainment, target-setting, incentive and reward structures and information feedback loops.
(Kloot & Martin, 2000)	Performance Management	The case of local government	Highlighted a suggested framework for strategic and balanced local government performance measurement.
(W. Van Grembergen, 2000)	Performance Management	A case study of a bank	If use a cascade of scorecards linking Business BSC to IT BSC and then to IT strategic, IT development and IT operational scorecards, IT governance measures and concerns will be identified to top management • Identifies key components of development and strategic IT BSC for a bank.
(Guldentops, E., Van Grembergen, W., & De Haes, 2002)	Performance Management	Survey of CobIT users	Discussed the maturity model process and the results of a survey of CobiT users.
(Lam, 2003)	Performance Management	A case study of a bank	Discussed how the IT balanced scorecard (ITBSC) can be linked to the business balanced scorecard (BBSC) to support IT/business governance and alignment processes.
(Warland & Ridley, 2005a)	Performance Management	Semi-structured interviews with 9 participants from three Tasmanian Government Agencies	Discussed the awareness and understanding of IT Control frameworks ie CobiT, ITIL etc.
(Dahlberg & Kivijärvi, 2006)	Performance Management	27 public/private sector organization	Developed a new integrative IT governance framework and an assessment tool to measure ITG effectiveness.
(Dahlberg & Lahdelma, 2007)	Performance Management	109 senior executives from 20 enterprises	Examined the role of ITG maturity evaluations by senior executives and their links to outsourcing.
(Verbeeten, 2008a)	Performance Management	Case in public sector organizations	Investigated whether performance management practices affect performance in public sector organizations.

continued on following page

Table 2. Continued

Theoretical Framework	ITG Focus Area	Empirical/Case Study	Research Summary
(Ferreira & Otley, 2009)	Performance Management	2 cases studies (Portuguese Post Office, and s Texco, a medium-sized company)	Put forward the performance management systems framework as a research tool for describing the structure and operation of performance management systems (PMSs) in a more holistic manner.
(Moynihan & Pandey, 2010)	Performance Management	Data collected a multimethod study of the National Administrative Studies Project (NASP-IV)	Proposed that understanding public employee use of performance information is perhaps the most pressing challenge for scholarship on performance management.
(Nfuka & Rusu, 2011)	Performance Management	Sample data from Tanzanian public sector organizations	Analysed the effect of critical success factors (CSFs) on information technology (IT) governance performance in public sector organizations in a developing country such as Tanzania.
(Mohamed & Singh, 2012)	Performance Management	A systematic literature	Developed a conceptual framework that examines information technology (IT) governance effectiveness, its determinants, and its impacts on private organizations.
(Ates, Garengo, Cocca, & Bititci, 2013)	Performance Management	literature review and multiple case studies in 37 European SMEs	Examined the gap between performance management theory and practice in small and medium-sized enterprises (SMEs) and analyzed it in the light of the specific characteristics and needs of SMEs, in order to identify how SMEs can develop their managerial practices for effective performance management.
(Bermejo, Tonelli, Zambalde, Santos, & Zuppo, 2014)	Performance Management	Data were collected from 652 Brazilian companies	Indicated how companies can succeed in terms of IT governance practices and has potential gaps based on organizations with weaker IT and business results.
(Dooren, Bouckaert, & Halligan, 2015)	Performance Management	Case studies from the UK and Australian public sectors organizations	Developed a comprehensive understanding of performance management as a concept and the phenomenon that has swept OECD (Organisation for Economic Co-operation and Development) countries, to examine how it has been applied in practice and to examine the relationship with public management and public policy.
(Gerrish, 2016)	Performance Management	No data	Conducted a meta-analysis on the impact of performance management on performance in public organizations. It contributes to the current literature in three ways.
(Mirghafoori, Andalib, & Keshavarz, 2017)	Performance Management	A case study in the Manufacturing Industry	Investigated the positive effects of supply chain agility on green performance in the Yazd ceramic tile manufacturing industry.

DISCUSSION AND FUTURE DIRECTIONS

In the prior section, research across the five focus areas was presented. The research in these focus areas has been performed in relative isolation and whilst this research contributes to the overall understanding of the key components of IT governance, it has not adopted a holistic viewpoint.

- For ITG to become an accepted part of organizational governance processes in the same way that corporate governance has been accepted, ITG research needs to develop models which encompass all focus areas of ITG. The models would also need to incorporate measurement methods which could be based on prior research in performance measurement. A number of researchers including (Dahlberg & Kivijärvi, 2006; De Haes & Van Grembergen, 2005b; Peterson, 2004) have attempted to develop holistic ITG models but there is still much room for improvement in fusing ITG into one process. A study by (Bowen, Chew, & Hash, 2007) explored the factors influencing IT governance structures, processes and outcome metrics and builds a model which relates these factors to ITG effectiveness. The importance of IS strategy in business has been studied by numbers of scholars. (Olson, 2008) underlined the information strategy as one of the components of a strategy pyramid and operations in an organization. Chen (2010) examined the relationship between the alignment maturity dimensions and IS strategic alignment. The alignment maturity of companies in China was assessed to provide a snapshot of business–IT alignment in China. In their survey, (Bradley, Pratt, Byrd, Outlay & Wynn Jr, 2012) argued that enterprise architecture maturity indirectly influences the effectiveness of IT resources when IT alignment is incorporated as a mediating variable.

In another study, (Alaceva & Rusu, 2015) Showed that low understanding of counterpart's environment; poor communication; unclear specifications; limited cooperation and lack of mutual commitment and support inhibits the achievement of alignment between business and IT domains on the social dimension. (Renaud et al., 2016) proposed an explanation for practitioners' apparent failures to fulfill SAM's intended contribution.

In recent works, Goni et al. (2017) underscored the important role of information systems during the sustainability implementation. (Huygh, Haes, Joshi, & Grembergen, 2018) presented the results of an analysis into which governance and management of IT processes are leveraged in practice for answering two key global IT management concerns: alignment and security.

- Research on the IT delivery value has had a similar focus to strategic alignment research with a number of models and frameworks developed. There have been two key issues studied within this focus area: (1) distinguishing between the potential value and realizable value of IT systems and (2) the link between organizational performance and delivery of value from IT systems. As with strategic alignment research, there has been little focus on the testing of these models. Development of practical methods for organizations to improve their understanding of value delivery and their ability to measure it effectively would make an important contribution to research in this area. Whilst the prior research of Menon and Lee (2000), McKay et al. (2003), Weill and Ross (2004), and Gregor et al. (2006) has provided a greater understanding of value delivery processes, further work is needed to extend knowledge on this issue. (Heier, Borgman & Mervyn, 2007) Considers the impact of ITG software on value delivery from IT systems, and examines the relationship between ITG applications, ITG processes and value delivery from IT. In another work, (Nazımoğlu & Özsen, 2010) defined and analyze risks within information technologies (IT) in service delivery. Some specific risks that appear in IT service delivery and the relationships between risks will be defined.

In recent works, Beloglazov et al. (2014) created a design artifact for building product lines of IT service delivery simulation models, which vastly simplify and reduce the cost of simulation model design and development. Tsai et al. (2015) produced an effective measure of ERP performance in an ITG framework, and provided evidence of partial mediation effects of value delivery between service quality and ERP performance. Vlietland et al. (2016) supported enterprises that suffer from such dependencies with a governance framework that helps them mitigate collaboration issues between sets of codependent Scrum teams. Benaroch and Chernobai (2017) demonstrated that subsequent to experiencing operational IT failures firms make improvements to the IT competency level of their boards, and the improvements are proportional to the degree of negative market reaction.

- IT resources management has been an extensive area of IT governance research. Much of the research has focused on the best type of IT resource structure for an organization. Other key outcomes of the research in this focus area have been the development of broader models of ITG (Karimi, Bhattacharjee, Gupta & Somers, 2000; Schwarz & Hirschheim, 2003; Peterson, 2004; Van Grembergen & De Haes, 2009). In other works, Chênevert and Tremblay (2009) revealed that the use of an extensive relational empowerment strategy is significantly and negatively related to voluntary turnover when accompanied by a compensation program that rewards performance. Lengnick-Hall et al. (2011) proposed that an organization's capacity for resilience is developed through strategically managing human resources to create competencies among core employees, that when aggregated at the organizational level, make it possible for organizations to achieve the ability to respond in a resilient manner when they experience severe shocks. Maes, De Haes, and Van Grembergen (2013) proposed a case study in order to identify multiple business case tasks that complement the process of Peppard, Ward, and Daniel (2007).

In recent works, Wiedemann et al. (2015) identified critical success factors for IT service delivery ITSD management. Hagen and Bouchard (2016) identifies portions of the literature in the areas of Information Technology (IT) management, skills development, and curriculum development that support the design of a holistic conceptual framework for instruction in non-technical skills within the IT higher education context. Altemimi and Zakaria (2017) identified the domain of IT governance and provide insights practice with each domain that was detected through literature.

- Risk management of IT systems research has focused on three main areas. These are identification of IT risks, risk management models and frameworks and risk assessment processes. The identification of risks research has provided an important understanding of outsourcing, IT projects and security risks. The development of an integrated model of risk management by Young and Jordan (2002) has made an important contribution to this focus area. Development of models/frameworks extending this work would broaden the knowledge of IT risk management processes. Studies that identify practical methods that organizations could use to improve their IT risk management processes and better assess IT risks would also be beneficial (Spira

& Page, 2003). Gewalt and Helbig (2006) developed a governance model for mitigating outsourcing risks. The proposed model consists of strategic direction, governance principles and organizational structures. By examining stock market reactions to the announcement of operational losses by financial companies, Gillet et al. (2010) attempted to disentangle operational losses from reputational damage. The proposed analysis deals with 154 events coming from the FIRST database of OpVantage. In recent works, Ellul and Yerramilli (2013) suggested that a strong and independent risk management function can curtail tail risk exposures at banks. Lam (2014) addresses the key concepts, processes, and tools underlying risk management, and lays out clear strategies to manage what is often a highly complex issue. Brustbauer (2016) suggested that SMEs follow either an active or a passive ERM approach, which affects their strategic orientation; a passive approach results in a defensive strategy and an active approach, an offensive strategy. Hopkinson (2017) described the issues facing anyone tasked with assessing project risk management capability.

- Research on IT performance management has predominantly focused on measurement processes including maturity models and IT balanced scorecard methods (Dahlberg & Kivijärvi, 2006; Dahlberg & Lahdelma, 2007; Guldentops, Van Grembergen & De Haes, 2002; Kloot & Martin, 2000; Lam, 2003; Van Grembergen, 2000; Verbeeten, 2008b; Warland & Ridley, 2005b). In recent works, (Ates et al., 2013) investigated the gap between theory and practice in performance management in small and medium-sized enterprises (SMEs) and analyze it in the light of specific SME characteristics and needs, to identify how SMEs can develop their managerial practice for effective performance management. Bermejo et al. (2014) indicated how businesses can be successful in terms of IT governance practices, and it presents potential deficiencies based on organizations with lower IT and business results. Gerrish (2016) conducted a meta-analysis on the impact of performance management on performance in public organizations. It contributes to the current literature in three ways. Mirghafoori et al. (2017) investigated the positive effects of supply chain agility on green performance in the Yazd ceramic tile manufacturing industry.

Possible research directions, which could be considered in the future for each focus area, are described in Table 3.

Table 3. Future directions on IT governance

IT Governance Area	Future Direction
IT alignment	<ul style="list-style-type: none"> • To achieve greater maturity in decision-making structures and processes within organizations, research must focus primarily on developing appropriate practices that create synergy between IT staff and business management. • Research should focus on IT investment issues and its impact on strategic business alignment. • Aligning Organizational Capabilities of Information Governance in the Age of New Technologies such as Big Data and the Internet of Things.
Value delivery	<ul style="list-style-type: none"> • Study the value brought by agility and agile methods such as DevOps on organizational governance.
Resources management	<ul style="list-style-type: none"> • Determine the relevance and differences in competency requirements for non-IT executives and other non-IT disciplines on the Board of Directors.
Risk management	<ul style="list-style-type: none"> • Determine the relationship between board information and technology risk monitoring and director competence. Such research could focus on risk reduction, based on timely decision making and the quality of decisions. • Measure the influence of the enterprise risk management function on decision making in the organization.
Performance management	<ul style="list-style-type: none"> • Identify factors that contribute to the performance of enterprise systems steering committees in implementing successful technology solutions across the enterprise.

CONCLUSION

This chapter has attempted to establish guidelines for future research based on a classification and analysis of IT governance frameworks for large organizations. The review and analysis of the ITG frameworks were organized using the five key components identified by COBIT 5. It drew on a wider range of documents that are usually found in some reviews, and the following conclusions were drawn. IT governance research faces the need to develop a comprehensive ITG framework that systematically builds on the different IG definitions proposed so far. This study would encourage future work to seek to develop or build on, some form of an integrated ITG framework this would both guide case study and other features of specific bodies and contribute to an evolving tradition of academic analysis. In addition, ITG executives suggested by research must take into account companies' requirements and challenges in terms of efficiency, added value, risk management and reputation, as they will facilitate internal audit and compliance with international standards at a strategic level and promote companies' competitiveness. To better evaluate IT governance frameworks and best practices, we will detail the different standards proposed in the literature in the next chapter.

REFERENCES

- Aasi, P., Rusu, L., & Han, S. (2014). Culture Influence on IT Governance: What We Have Learned? *International Journal of IT/Business Alignment and Governance*, 5(1), 34–49. doi:10.4018/ijitbag.2014010103
- Aebi, V., Sabato, G., & Schmid, M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance*, 36(12), 3213–3226. doi:10.1016/j.jbankfin.2011.10.020
- Alaceva, C., & Rusu, L. (2015). Barriers in achieving business/IT alignment in a large Swedish company: What we have learned? *Computers in Human Behavior*, 51, 715–728. doi:10.1016/j.chb.2014.12.007
- Ali, S., & Green, P. (2009). IT governance mechanisms in public sector organisations: An Australian context. *Handbook of Research on Information Management and the Global Landscape*, 458–478.
- Ali, S., Green, P., & Robb, A. (2015). Information technology investment governance: What is it and does it matter? *International Journal of Accounting Information Systems*, 18, 1–25. doi:10.1016/j.accinf.2015.04.002
- Altemimi, M. A. H., & Zakaria, M. S. (2017). *An Approach Towards Assessing Effective IT Governance Setting: Malaysia Public Sector Case Study BT - Leadership, Innovation and Entrepreneurship as Driving Forces of the Global Economy*. Cham: Springer International Publishing.
- Ates, A., Garengo, P., Cocca, P., & Bititci, U. (2013). The development of SME managerial practice for effective performance management. *Journal of Small Business and Enterprise Development*, 20(1), 28–54. doi:10.1108/14626001311298402
- Avison, D., Jones, J., Powell, P., & Wilson, D. (2004). Using and validating the strategic alignment model. *The Journal of Strategic Information Systems*, 13(3), 223–246. doi:10.1016/j.jsis.2004.08.002
- Bailey, A., Minto-Coy, I., & Thakur, D. (2017). *IT Governance in E-Government Implementations in the Caribbean: Key Characteristics and Mechanisms BT - Information Technology Governance in Public Organizations: Theory and Practice*. Cham: Springer International Publishing; doi:10.1007/978-3-319-58978-7_9

Bart, C., & Turel, O. (2010). IT and the Board of Directors: An Empirical Investigation into the “Governance Questions” Canadian Board Members Ask about IT. *Journal of Information Systems*, 24(2), 147–172. doi:10.2308/jis.2010.24.2.147

Beloglazov, A., Banerjee, D., Hartman, A., & Buyya, R. (2014). Improving Productivity in Design and Development of Information Technology (IT) Service Delivery Simulation Models. *Journal of Service Research*, 18(1), 75–89. doi:10.1177/1094670514541002

Benaroch, M., & Chernobai, A. (2017). Operational IT Failures, IT Value Destruction, and Board-Level IT Governance Changes. *Management Information Systems Quarterly*, 41(3), 729–762. doi:10.25300/MISQ/2017/41.3.04

Bermejo, P. H. de S., Tonelli, A. O., Zambalde, A. L., dos Santos, P. A., & Zuppo, L. (2014). Evaluating IT Governance Practices and Business and IT Outcomes: A quantitative Exploratory Study in Brazilian Companies. *Procedia Technology*, 16, 849–857. doi:10.1016/j.protcy.2014.10.035

Blanger, J. P. (2013). La non gouvernance documentaire: Quels risques pour l’organisation? *Documentaliste*, 50(1), 56–57.

Bowen, P., Chew, E., & Hash, J. (2007). *Information Security Guide For Government Executives Information Security Guide For Government Executives*. National Institute of Standards and Technology NIST. doi:10.6028/NIST.IR.7359

Bradley, R. V., Pratt, R. M., Byrd, T. A., Outlay, C. N., & Wynn, D. E. Jr. (2012). Enterprise architecture, IT effectiveness and the mediating role of IT alignment in US hospitals. *Information Systems Journal*, 22(2), 97–127. doi:10.1111/j.1365-2575.2011.00379.x

Brown, A. E., Grant, G. G., & Sprott, E. (2005a). Framing the Frameworks: A Review of It Governance Research. *Communications of the Association for Information Systems*, 15, 696–712.

Brown, A. E., Grant, G. G., & Sprott, E. (2005b). Framing the Frameworks: A Review of It Governance Research. *Communications of the Association for Information Systems*, 15(May), 696–712.

Brown, W. A., Laird, R., Gee, C., & Mitra, T. (2008). *SOA governance: achieving and sustaining business and IT agility*. Pearson Education.

Bruce, K. (1998). Can you align IT with business strategy? *Strategy and Leadership*, 26(5), 16–20. doi:10.1108/eb054620

Brustbauer, J. (2016). Enterprise risk management in SMEs: Towards a structural model. *International Small Business Journal*, 34(1), 70–85. doi:10.1177/0266242614542853

Carter, C. B., & Lorsch, J. W. (2004). *Back to the drawing board: Designing corporate boards for a complex world*. Harvard Business Press.

Cater-Steel, A. (2009). *Information Technology Governance and Service Management: Frameworks and Adaptations*. IGI Global. doi:10.4018/978-1-60566-008-0

Charoensuk, S., Wongsurawat, W., & Khang, D. B. (2014). Business-IT Alignment: A practical research approach. *The Journal of High Technology Management Research*, 25(2), 132–147. doi:10.1016/j.hitech.2014.07.002

Chen, J.-S., Tsou, H. T., & Huang, A. Y.-H. (2009). Service Delivery Innovation: Antecedents and Impact on Firm Performance. *Journal of Service Research*, 12(1), 36–55. doi:10.1177/1094670509338619

Chen, L. (2010). Business–IT alignment maturity of companies in China. *Information & Management*, 47(1), 9–16. doi:10.1016/j.im.2009.09.003

Chênevert, D., & Tremblay, M. (2009). Fits in strategic human resource management and methodological challenge: Empirical evidence of influence of empowerment and compensation practices on human resource performance in Canadian firms. *International Journal of Human Resource Management*, 20(4), 738–770. doi:10.1080/09585190902770547

Cumps, B., Viaene, S., Dedene, G., & Vandenbulcke, J. (2006). An empirical study on business/ICT alignment in European organisations. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 8(C), 1–10. 10.1109/HICSS.2006.53

Dahlberg, T., & Kivijärvi, H. (2006). An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument. *39th Hawaii International Conference on System Sciences*, 0(C), 1–10. 10.1109/HICSS.2006.57

Dahlberg, T., & Lahdelma, P. (2007). IT governance maturity and IT outsourcing degree: An exploratory study. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. 10.1109/HICSS.2007.306

De Haes, S., & Van Grembergen, W. (2005a). IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 237b–237b. 10.1109/HICSS.2005.362

De Haes, S., & Van Grembergen, W. (2005b). IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 237b–237b. 10.1109/HICSS.2005.362

De Haes, S., & Van Grembergen, W. (2006). Information technology governance best practices in Belgian organisations. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 8. 10.1109/HICSS.2006.222

de Haes, S., & van Grembergen, W. (2009). An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment. *Information Systems Management*, 26(2), 123–137. doi:10.1080/10580530902794786

Dibbern, J., Goles, T., Hirschheim, R., & Jayatilaka, B. (2004). Information Systems Outsourcing: A Survey and Analysis of the Literature. *SIGMIS Database*, 35(4), 6–102. doi:10.1145/1035233.1035236

Dickinson, G. (2001). Enterprise Risk Management: Its Origins and Conceptual Foundation. *The Geneva Papers on Risk and Insurance. Issues and Practice*, 26(3), 360–366. doi:10.1111/1468-0440.00121

Dong, X., Liu, Q., & Yin, D. (2008). Business Performance, Business Strategy, and Information System Strategic Alignment: An Empirical Study on Chinese Firms. *Tsinghua Science and Technology*, 13(3), 348–354. doi:10.1016/S1007-0214(08)70056-7

EASA. (2016). *Practices for risk-based oversight*. EASA.

El-Mekawy, M., Rusu, L., & Perjons, E. (2015). An evaluation framework for comparing business-IT alignment models: A tool for supporting collaborative learning in organizations. *Computers in Human Behavior*, 51, 1229–1247. doi:10.1016/j.chb.2014.12.016

- Elhasnaoui, S., Medromi, H., Chakir, A., & Sayouti, A. (2015). A new IT Governance architecture based on multi agents system to support project management. *2015 International Conference on Electrical and Information Technologies (ICEIT)*, 43–46. 10.1109/EITech.2015.7162957
- Ellul, A., & Yerramilli, V. (2013). Stronger risk controls, lower risk: Evidence from US bank holding companies. *The Journal of Finance*, 68(5), 1757–1803. doi:10.1111/jofi.12057
- Felix, R., Rauschnabel, P. A., & Hinsch, C. (2017). Elements of strategic social media marketing: A holistic framework. *Journal of Business Research*, 70, 118–126. doi:10.1016/j.jbusres.2016.05.001
- Ferreira, A., & Otley, D. (2009). The design and use of performance management systems: An extended framework for analysis. *Management Accounting Research*, 20(4), 263–282. doi:10.1016/j.mar.2009.07.003
- Gerrish, E. (2016). The Impact of Performance Management on Performance in Public Organizations: A Meta-Analysis. *Public Administration Review*, 76(1), 48–66. doi:10.1111/puar.12433
- Gewald, H., & Helbig, K. (2006). A Governance Model for Managing Outsourcing Partnerships. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, 8(C), 194.3. Retrieved from <http://www.computer.org/plugins/dl/pdf/proceedings/hicss/2006/2507/08/250780194c.pdf?template=1&loginState=1&userData=anonymous-IP%253A%253A130.89.229.171>
- Gillet, R., Hübner, G., & Plunus, S. (2010). Operational risk and reputation in the financial industry. *Journal of Banking & Finance*, 34(1), 224–235. doi:10.1016/j.jbankfin.2009.07.020
- Gold, R. S. (2002). Enabling the strategy-focused IT organization. *Information Systems Control Journal*, 4, 21–24.
- Goni, F. A., Chofreh, A. G., Mukhtar, M., Sahran, S., Shukor, S. A., & Klemeš, J. J. (2017). Strategic alignment between sustainability and information systems: A case analysis in Malaysian public Higher Education Institutions. *Journal of Cleaner Production*, 168, 263–270. doi:10.1016/j.jclepro.2017.09.021
- Grant, G., & Tan, F. B. (2013). Governing IT in inter-organizational relationships: Issues and future research. *European Journal of Information Systems*, 22(5), 493–497. doi:10.1057/ejis.2013.21

Gregor, S., Martin, M., Fernandez, W., Stern, S., & Vitale, M. (2006). The transformational dimension in the realization of business value from information technology. *The Journal of Strategic Information Systems*, 15(3), 249–270. doi:10.1016/j.jsis.2006.04.001

Grover, V., & Kohli, R. (2012). Cocreating IT value: New capabilities and metrics for multifirm environments. *Management Information Systems Quarterly*, 36(1), 225–232.

Guldentops, E., Van Grembergen, W., & De Haes, S. (2002). Control and governance maturity survey: Establishing a reference benchmark and a self assessment tool. *Information Systems Control Journal*, 6, 32–35.

Hagen, M., & Bouchard, D. (2016). *Developing and Improving Student Non-Technical Skills in IT Education: A Literature Review and Model*. Informatics. doi:10.3390/informatics3020007

Heier, H., Borgman, H. P., & Mervyn, G. M. (2007). Examining the relationship between IT governance software and business value of IT: Evidence from four case studies. *Proceedings of the 40th Hawaii International Conference on System Sciences*.

Hirschheim, R., & Sabherwal, R. (2001). Detours in the Path toward Strategic Information Systems Alignment. *California Management Review*, 44(1), 87–108. doi:10.2307/41166112

Hopkinson, M. (2017). *The Project Risk Maturity Model: Measuring and improving risk management capability*. London: Routledge. doi:10.4324/9781315237572

Hoyt, R. E., & Liebenberg, A. P. (2011). The Value of Enterprise Risk Management. *The Journal of Risk and Insurance*, 78(4), 795–822. doi:10.1111/j.1539-6975.2011.01413.x

Hsieh, J. J. P.-A., Rai, A., & Xu, S. X. (2011). Extracting Business Value from IT: A Sensemaking Perspective of Post-Adoptive Use. *Management Science*, 57. doi:10.1287/mnsc.1110.1398

Huygh, T., De Haes, S., Joshi, A., & Van Grembergen, W. (2018). Answering key global IT management concerns through IT governance and management processes : A COBIT 5 View. *Hawaii International Conference on System Sciences*, 9(1), 5335–5344.

ITGI. (2003). *Board Briefing on IT Governance*. ITGI.

Joshi, A., Bollen, L., Hassink, H., De Haes, S., & Van Grembergen, W. (2018). Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. *Information & Management*, 55(3), 368–380. doi:10.1016/j.im.2017.09.003

Jules, A. (2014). *La gouvernance de l'information dans les organisations*.

Kaen, F. R. (2005). Risk Management, Corporate Governance and the Public Corporation BT - Risk Management: Challenge and Opportunity. Berlin: Springer Berlin Heidelberg; doi:10.1007/3-540-26993-2_21

Kaplan, R. S., & Norton, D. P. (1992). Search of Excellence—der Maßstab muß neu definiert werden. *Harvard Manager*, 14(4), 37–46.

Karimi, J., Bhattacharjee, A., Gupta, Y. P., & Somers, T. M. (2000). The effects of MIS steering committees on information technology management sophistication. *Journal of Management Information Systems*, 17(2), 207–230. doi:10.1080/07421222.2000.11045641

Kloot, L., & Martin, J. (2000). Strategic performance management: A balanced approach to performance management issues in local government. *Management Accounting Research*, 11(2), 231–251. doi:10.1006/mare.2000.0130

Kooper, M. N., Maes, R., & Lindgreen, E. E. O. R. (2011). On the governance of information: Introducing a new concept of governance to support the management of information. *International Journal of Information Management*, 31(3), 195–200. doi:10.1016/j.ijinfomgt.2010.05.009

Korac-Kakabadse, N., & Kakabadse, A. (2001). IS/IT governance: Need for an integrated model. *Corporate Governance: The International Journal of Business in Society*, 1(4), 9–11. doi:10.1108/EUM0000000005974

Kwon, D., & Watts, S. (2006). IT valuation in turbulent times. *The Journal of Strategic Information Systems*, 15(4), 327–354. doi:10.1016/j.jsis.2006.07.003

Laeven, L., & Levine, R. (2009). Bank Governance, Regulation, and Risk Taking. *Journal of Financial Economics*, 93(2), 259–275. doi:10.1016/j.jfineco.2008.09.003

Lam, J. (2003). Enterprise. *Risk Management*, 115–131. doi:10.1080/10920277.2012.10590630

Lam, J. (2014). *Enterprise risk management: from incentives to controls*. John Wiley & Sons. doi:10.1002/9781118836477

From Information Governance to IT Governance

Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review*, 21(3), 243–255. doi:10.1016/j.hrmr.2010.07.001

Luftman, J. (2003). Assessing It/Business Alignment. *Information Systems Management*, 20(4), 9–15. doi:10.1201/1078/43647.20.4.20030901/77287.2

Luftman, J., Papp, R., & Brier, T. (1999). Enablers and Inhibitors of business-IT Alignment. *Commun. AIS*, 1(3es). Retrieved from <http://dl.acm.org/citation.cfm?id=374122.374123>

Maes, K., De Haes, S., & Van Grembergen, W. (2012). IT Value Management as a Vehicle to Unleash the Business Value from IT Enabled Investments. *International Journal of IT/Business Alignment and Governance*, 3(1), 47–62. doi:10.4018/jitbag.2012010103

Maes, K., De Haes, S., & Van Grembergen, W. (2013). Investigating a Process Approach on Business Cases: An Exploratory Case Study at Barco. *International Journal of IT/Business Alignment and Governance*, 4(2), 37–53. doi:10.4018/ijitbag.2013070103

Magnusson, J. (2010). *Professional Analysts and the Ongoing Construction of IT Governance*. Academic Press. doi:10.4018/jitbag.2010040101

McKay, J., Marshall, P., & Smith, L. (2003). Steps Towards Effective IT Governance: Strategic IT Planning, Evaluation and Benefits Management. *Pacific Asia Conference on Information Systems*, 956–970. Retrieved from <http://www.pacis-net.org/file/2003/papers/is-strategy/214.pdf>

Menon, N. M., & Lee, B. (2000). Cost control and production performance enhancement by IT investment and regulation changes: Evidence from the healthcare industry. *Decision Support Systems*, 30(2), 153–169. doi:10.1016/S0167-9236(00)00095-6

Mills, K., Viaene, S., & Ribbers, P. (2006). On how the feasibility study is influenced by an ICT project's main trigger. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 8(C), 1–10. 10.1109/HICSS.2006.363

Mirghafoori, S. H., Andalib, D., & Keshavarz, P. (2017). Developing Green Performance Through Supply Chain Agility in Manufacturing Industry: A Case Study Approach. *Corporate Social Responsibility and Environmental Management*, 24(5), 368–381. doi:10.1002/csr.1411

Mohamed, N., & Singh, J. K. (2012). A conceptual framework for information technology governance effectiveness in private organizations. *Information Management & Computer Security*, 20(2), 88–106. doi:10.1108/09685221211235616

Moynihan, D. P., & Pandey, S. K. (2010). The Big Question for Performance Management: Why Do Managers Use Performance Information? *Journal of Public Administration: Research and Theory*, 20(4), 849–866. doi:10.1093/jopart/muq004

Murphy, K., Lyytinen, K., & Somers, T. (2018). A Socio-Technical Model for Project-Based Executive IT Governance. *Proceedings of the 51st Hawaii International Conference on System Sciences | 2018 A*, 9, 4825–4834.

Nazımoğlu, Ö., & Özsen, Y. (2010). Analysis of risk dynamics in information technology service delivery. *Journal of Enterprise Information Management*, 23(3), 350–364. doi:10.1108/17410391011036102

Nfuka, E. N., & Rusu, L. (2011). The effect of critical success factors on IT governance performance. *Industrial Management & Data Systems*, 111(9), 1418–1448. doi:10.1108/02635571111182773

Olson, E. G. (2008). Creating an enterprise-level “green” strategy. *The Journal of Business Strategy*, 29(2), 22–30. doi:10.1108/02756660810858125

Olson, D. L. (2015). *Enterprise risk management in finance*. Springer.

Otley, D. (1999). Performance management: A framework for management control systems research. *Management Accounting Research*, 10(4), 363–382. doi:10.1006/mare.1999.0115

Pang, M.-S. (2014). IT governance and business value in the public sector organizations — The role of elected representatives in IT governance and its impact on IT value in U.S. state governments. *Decision Support Systems*, 59, 274–285. doi:10.1016/j.dss.2013.12.006

Peppard, J., Ward, J., & Daniel, E. (2007). Managing the realization of business benefits from IT investments. *MIS Quarterly Executive*, 6(1).

PerreinJ.-P. (2014). *3org*. Retrieved from www.3org.com

Peterson, R. (2004). Crafting information technology governance. *Information Systems Management*, 21(4), 7–22. doi:10.1201/1078/44705.21.4.20040901/84183.2

Peterson, R., Parker, M., Ribbers, P., Peterson, R. R., & Parker, M. M. (2002). Information Technology Governance Processes Under Environmental Dynamism: Investigating Competing Theories of Decision Making and Knowledge Sharing. *ICIS 2002 Proceedings*, 562–575.

Peterson, R. R. (2001). Configurations and coordination for global information technology governance: Complex designs in a transnational european context. *Proceedings of the Hawaii International Conference on System Sciences*, 0(c), 217. 10.1109/HICSS.2001.927133

Ploesser, K., Recker, J., & Rosemann, M. (2008). Towards a Classification and Lifecycle of Business Process Change A Classification and Lifecycle of Process Change Strategies. *BPMDs'08: Business Process Life-Cycle: Design, Deployment, Operation & Evaluation, 2008*, 10–18.

Reich, B. H., & Benbasat, I. (2000). Factors That Influence the Social Dimension of Alignment between Business and Information Technology Objectives. *Management Information Systems Quarterly*, 24(1), 81–113. doi:10.2307/3250980

Renaud, A., Walsh, I., & Kalika, M. (2016). Is SAM still alive? A bibliometric and interpretive mapping of the strategic alignment research field. *The Journal of Strategic Information Systems*, 25(2), 75–103. doi:10.1016/j.jsis.2016.01.002

Rezaee, Z., & Reinstein, A. (1998). The impact of emerging information technology on auditing. *Managerial Auditing Journal*, 13(8), 465–471. doi:10.1108/02686909810236271

Sambamurthy, V., & Zmud, R. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies. *Management Information Systems Quarterly*, 23(2), 261–290. doi:10.2307/249754

Sauvajol-Rialland, C. (2010). A surcharge informationnelle dans l'organisation: les cadres au bord de la «crise de nerf». *Magazine de la Communication de crise et sensible*, 19.

Scholl, H. J., Kubicek, H., & Cimander, R. (2011). Interoperability, enterprise architectures, and IT governance in government. *Lecture Notes in Computer Science*, 6846, 345–354. doi:10.1007/978-3-642-22878-0_29

Schwarz, A., & Hirschheim, R. (2003). An extended platform logic perspective of IT governance: Managing perceptions and activities of IT. *The Journal of Strategic Information Systems*, 12(2), 129–166. doi:10.1016/S0963-8687(03)00021-0

Siatiras, K. (2013). Information governance: New approach or old news? *IQ: The RIM Quarterly*, 29(2), 26.

Simonsson, M., & Johnson, P. (2006). Defining IT governance—a consolidation of literature. In *The 18th conference on advanced information systems engineering* (Vol. 6). Academic Press.

Simonsson, M., & Johnson, P. (2006). Assessment of IT Governance - A Prioritization of Cobit. *Proceedings of the Conference on Systems Engineering Research*. Retrieved from <http://sse.stevens.edu/fileadmin/cser/2006/papers/151-Simonsson-Assessment of IT Governance.pdf>

Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16(4), 640–661. doi:10.1108/09513570310492335

Spohrer, J., & Maglio, P. P. (2008). The emergence of service science: Toward systematic service innovations to accelerate co-creation of value. *Production and Operations Management*, 17(3), 238–246. doi:10.3401/poms.1080.0027

Tsai, W.-H., Chou, Y.-W., Leu, J.-D., Chen, D. C., & Tsaur, T.-S. (2015). Investigation of the mediating effects of IT governance-value delivery on service quality and ERP performance. *Enterprise Information Systems*, 9(2), 139–160. doi:10.1080/17517575.2013.804952

Turel, O., & Bart, C. (2014). Board-level IT governance and organizational performance. *European Journal of Information Systems*, 23(2), 223–239. doi:10.1057/ejis.2012.61

Valentine, E. L. H. (2016). *Enterprise technology governance: new information and technology core competencies for boards of directors* (Doctoral Dissertation). Queensland University of Technology. doi:10.13140/RG.2.2.34027.95529

From Information Governance to IT Governance

Van Dooren, W., Bouckaert, G., & Halligan, J. (2015). Performance Management in the Public Sector. *Performance Management in the Public Sector*, 208. doi:10.13140/2.1.2299.9682

Van Grembergen, W. (2000). The balanced scorecard and IT governance. *International Conference on Challenges of Information Technology Management in the 21st Century*, 1123–1124.

Van Grembergen, W. (Ed.). (2004). Strategies for information technology governance. IGI Global.

Van Grembergen, W. (2013). Introduction to the Minitrack “IT Governance and its Mechanisms”-HICSS 2013. *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, 9, 4394–4394. 10.1109/HICSS.2007.292

Van Grembergen, W., & De Haes, S. (2009). *Enterprise governance of information technology: achieving strategic alignment and value*. Springer Science & Business Media.

Van Greuning, H., & Brajovic Bratanovic, S. (2009). *Analyzing Banking Risk: A framework for assessing corporate governance and financial risk management*. Academic Press. doi:10.1596/0-8213-4417-X

Van Lier, J., & Dohmen, T. (2007). Benefits management and strategic alignment in an IT outsourcing context. *Proceedings of the Annual Hawaii International Conference on System Sciences*. 10.1109/HICSS.2007.105

Verbeeten, F. H. M. (2008). Performance management practices in public sector organizations. *Accounting, Auditing & Accountability Journal*, 21(3), 427–454. doi:10.1108/09513570810863996

Verhoef, C. (2007). Quantifying the effects of IT-governance rules. *Science of Computer Programming*, 67(2–3), 247–277. doi:10.1016/j.scico.2007.01.010

Vlietland, J., van Solingen, R., & van Vliet, H. (2016). Aligning codependent Scrum teams to enable fast business value delivery: A governance framework and set of intervention actions. *Journal of Systems and Software*, 113, 418–429. doi:10.1016/j.jss.2015.11.010

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. doi:10.1016/j.cose.2013.04.004

Wang, D., & Liu, C. (2009). Model-based vulnerability analysis of IMS network. *Journal of Networks*, 4(4), 254–262. doi:10.4304/jnw.4.4.254-262

Wang, N., Xue, Y., Liang, H., & Ge, S. (2011). The Road to Business-IT Alignment: A Case Study of Two Chinese Companies. *Communications of AIS*, 2011(28), 415–436. Retrieved from <http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=70400209&S=R&D=buh&EbscoContent=dGJyMNLe80Sep7A4yOvqOLCmr0qeprJSsai4TLswxWXS&ContentCustomer=dGJyMPGnr0m0r7JJuePfgex44Dt6fIA%5Cnhttp://www.redi-bw.de/db/ebsco.php/search.ebscohost.com/login.aspx?d>

Warland, C., & Ridley, G. (2005). Awareness of IT Control Frameworks in an Australian State Government: A Qualitative Case Study. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 0(C), 236b–236b. 10.1109/HICSS.2005.116

Webb, P., Pollard, C., & Ridley, G. (2006). Attempting to define IT governance: Wisdom or folly? *Proceedings of the Annual Hawaii International Conference on System Sciences*, 8(C), 1–10. 10.1109/HICSS.2006.68

Weill, P., & Ross, J. (2005). A Matrixed Approach to Designing IT Governance. *MIT Sloan Management Review*, 46(2), 26–34. doi:10.1177/0275074007310556

Weill, P., & Ross, J. W. (2004). *How Top Performers Manage IT Decisions Rights for Superior Results*. In *IT Governance* (pp. 1–10). Harvard Business School Press. doi:10.2139srn.664612

Weill, P., & Woodham, R. (2002). *Don't Just Lead, Govern: Implementing Effective IT Governance*. CISR Working Paper, 17. doi:10.2139srn.317319

Wiedemann, A., Weeger, A., & Gewalt, H. (2015). Organizational structure vs. capabilities: Examining critical success factors for managing IT service delivery. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 4564–4574. 10.1109/HICSS.2015.544

Wipplinger, E. (2007). Philippe Jorion: Value at Risk – The New Benchmark for Managing Financial Risk. *Financial Markets and Portfolio Management*, 21(3), 397–398. doi:10.1007/11408-007-0057-3

Worthing, L., & Hendriks, J. (2010). *Une gestion documentaire réussie au sein du nouveau paradigme de l'information*. White Paper.

Xue, Y., Liang, H., & Boulton, W. R. (2008). Information Technology Governance in Information Technology Investment Decision Processes: The Impact of Investment Characteristics, External Environment, and Internal Context 1. *Management Information Systems Quarterly*, 32(1), 67–96. doi:10.2307/25148829

Young, R. C., & Jordan, E. (2002). IT Governance and Risk Management: an integrated multi-stakeholder framework. *Annual Meeting of Asian-Pacific Decision Sciences Institute*.

KEY TERMS AND DEFINITIONS

COBIT (Control Objectives for Information and Related Technologies): Links the objectives of the IS to those of the company in order to evaluate its maturity towards its IT: it is a tool for auditors. It represents a consensus among experts on good practices in IT governance and with regard to investments in IT and the service provided by the IT. It provides a measurement scale to diagnose possible slippages.

Information: An asset, like other business assets which have value to an organization and that needs to be suitably protected.

Information Systems: Defined as the deployment of information technology to collect, process and disseminate information in organizations and society. Employees using information technology are an important aspect of an information system. Information systems include both technological components and the humans who use them to store, process and distribute electronic data.

Performance Measurement: Keeps track and monitors the implementation of IT strategy, resource usage, IT process performance, IT project completion and service delivery.

Resource Management: The main focus on the optimal investment in IT.

Risk Management: The main focus on the risk control of the enterprise, transparency about the significant risks.

Strategic Alignment: The main focus on the connection and link between the IT strategy and business strategy also the business process with the IT operations.

Value Delivery: The main focus on if the IT delivers the value against the IT strategy, optimizing the IT cost and providing the intrinsic value of IT.

Chapter 2

A Deep Overview of Information Technology Governance Standards

ABSTRACT

This chapter presents the state of the art in research on the practice of information technology (IT) governance. The authors have chosen to present this state of the art by means of a frame of reference inspired by the four “worlds” framework that was initially introduced to characterize IT engineering problems. This framework, complemented by facets, provides a structure for characterizing governance approaches that facilitate their comparison. Each facet corresponds to an essential characteristic of IS governance. A facet is associated with a set of values that allow a finer comparison of approaches with each other. This chapter will provide a comprehensive understanding of the current state of IT governance standards and best practices.

INTRODUCTION

As information and communication technology develops, an increasing number of companies are recognizing the potential value of IT resources in delivering their firm’s strategic vision. IT is no longer a supporting tool for business, but a fundamental component of company strategy in such roles as operations, internal audit, compliance and decision support. A recent survey conducted by the IT Governance Institute (ITGI) with CEO/ CIOs drawn

DOI: 10.4018/978-1-5225-7826-0.ch002

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

from 22 countries shows that 87% of respondents agree that IT plays an important role in achieving company goals in the broadest sense (Simonsson & Johnson, 2006).

In recent years, leading international organizations have focused attention on effective corporate governance as means of improving the performance of firms' IT assets. These efforts have intensified in the wake of large-scale frauds such as Enron and WorldCom in the United States and shareholders ensuing dissatisfaction with companies. Multinationals and others have devised corporate governance structures to clarify and monitor the respective roles and responsibilities of shareholders, management, and employees. These structures have laid greater emphasis on the importance of IT assets and IT governance (ITG) structure, aiming to minimize financial risks on IT investment by providing transparency, accountability, and management processes. These criteria entail the effective allocation of IT resources in terms of clear structures and decision-making procedures for IT management. In this juncture, it has become imperative to redefine effective ITG, seeking to understand governance's role in aligning organizations' information assets with their strategic goals (Webb, Pollard, & Ridley, 2006). This alignment contributes to the creation of value in companies, through suggesting optimal amounts of risk for companies to take both in designing their management structures and in proactively responding to new business circumstances.

IT governance consists of structures, processes, and operational mechanisms that work together in harmony to ensure that IT investments and business objectives are aligned (De Haes & Van Grembergen, 2005). The cornerstone of IT governance is to provide decision-makers an acceptable level of assurance that an organization's strategic objectives are not jeopardized by IT failures (Benaroch & Chernobai, 2017). A conventional or, rather, inevitable approach for attaining a level of assurance includes the evaluation of the IT governance system in place. The evaluation was born of the need to assess the degree of conformation with standard practice through the utilization of methodologies and frameworks (Vlietland, van Solingen, & van Vliet, 2016). This in particular means that, by engaging in IT governance evaluation, organizations can periodically measure IT governance performance using well-proved worldwide frameworks or methods such as Control Objectives for Information and Related Technology (COBIT), IT Infrastructure Library ITIL, or the International Standards Organization's ISO 38500, to name few.

A range of research in literature examines IT governance structures and mechanisms (De Haes & Van Grembergen, 2005; Guldentops, Van Grembergen & De Haes, 2002; McKay, Marshall, & Smith, 2003; Ryan Peterson, Parker, Ribbers, Peterson, & Parker, 2002; Wim van Grembergen & de Haes, 2009). Explores factors inflecting adoption and implementation of IT governance systems (Aasi, Rusu & Han, 2014; Reich & Benbasat, 2000), and the use of codified frameworks and their impact on IT governance (El-Mekawy, Rusu, & Perjons, 2015; Guldentops, 2002; Wim van Grembergen & de Haes, 2009; Weber, 2014). The literature also indicates that, while there is widespread use of governance frameworks, there is a need for more research to investigate how these frameworks could be modified to fit a specific circumstance or context (Maleh, Zaydi, Sahid, & Ezzati, 2018). By the same token, aspects that involve the user behaviour in IT governance, although they have long been acknowledged (Grunwel & Sahama, 2016; Herath & Rao, 2009), have received far less attention from academics (Smits & Hillegersberg, 2015).

Several IT governance frameworks can guide the implementation of an IT governance program. Although frameworks and guidelines such as CobiT, ITIL, ValIT and ISO 38500 (Prieto-Diaz, 1991) have been widely adopted, there is no absolute standard IT governance framework; the combination that works best for an organization depends on business factors, corporate culture, IT maturity and staffing capacity. The level of implementation of these frameworks will also vary by organization.

This chapter presents the state of the art of research on the practice of information technology (IT) governance through an analysis of the various proposed standards. This analysis was conducted based on a meta-model of 4 words. This chapter is organized as follows: The first part describes the proposed reference framework for IT governance. Five recognized approaches are then evaluated under this framework. Finally, the chapter highlights the gaps in current approaches, our positioning with regard to the literature and its contribution to IT governance.

RESEARCH METHODOLOGY

This section proposes a meta-model to evaluate IT governance ITG approaches. This model is built around facets capturing a specific dimension of information governance. The principle of facets was introduced in Jarke, Mylopoulos, Schmidt, and Vassiliou (1992) for software engineering. This framework is

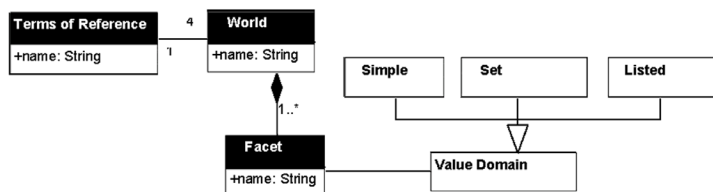
not intended to describe governance activities but to organize governance approaches along structuring analytical lines that seem relevant to us.

The framework is structured around four poles or “words”. The “four words” framework has been used in various engineering disciplines: IS engineering (Jarke & Pohl, 1993), requirements engineering (Rolland, 1998), process engineering (Nurcan & Rolland, 2003) and change engineering (Nehan & Deneckere, 2007). This framework has been used for the IT governance engineering and for component-based situational method engineering (Prieto-Diaz, 1991).

It is supplemented by facets according to the approach introduced in (“Information Security Governance: Guidance for Boards of Directors and Executive Management Guidance for Boards of Directors and Executive Management,” 2006). This aims to allow a more flexible and precise classification of software components and is based on the enumeration of component descriptors, their association with a lexicon of terms (thesaurus) and a graph of facets. The initial framework of the four words has been adapted by facets that are descriptive elements. Each facet can take a predefined value by a “value domain”:

- A simple value domain refers to a predefined primitive value type. This is the case of an integer or real value;
- An overall value domain (SET{a ;b ;...}) refers to a structured type. For example, a vector with n dimensions is a typically structured on n elements;
- A listed value domain (Enum{a, b,...}) refers to a listed type. Thus, a mention for a diploma is from a listed field and can take its value among the values defined on Enum{” Fairly Good “, ” Good “, ” Very Good “}

Figure 1. The proposed meta-model to evaluate IT governance frameworks



The meta-model in Figure 1 defines the proposed framework.

The reference framework is obtained by instantiating the metamodel described in Figure 1. The governance literature allows us to define the values taken by the attributes of the metamodel classes. The framework is presented in Figure 2 and comprises the following four words:

- The word “subject”. It presents IS governance as the object of analysis and identifies its intrinsic characteristics. Governance is described as an organizational structure for decision-making concerned with the simultaneous evolution of IT projects, business processes and IT processes.
- The word “use” is the purpose of ITG, it concerns the objectives of its users. In governance, CIOs make decisions with the objective of limiting risk, creating value and achieving a certain level of performance.
- The word “system” contains all the information useful to the activities of the ITG. It is the informational basis for decision making. It contains the elements for measuring ITG objectives as well as all the documents and models useful for sharing knowledge related to ITG.
- The word “development” consists of the processes of ITG. Their execution achieves the objectives of ITG and relies on the manipulation of the information elements of the ITG system.

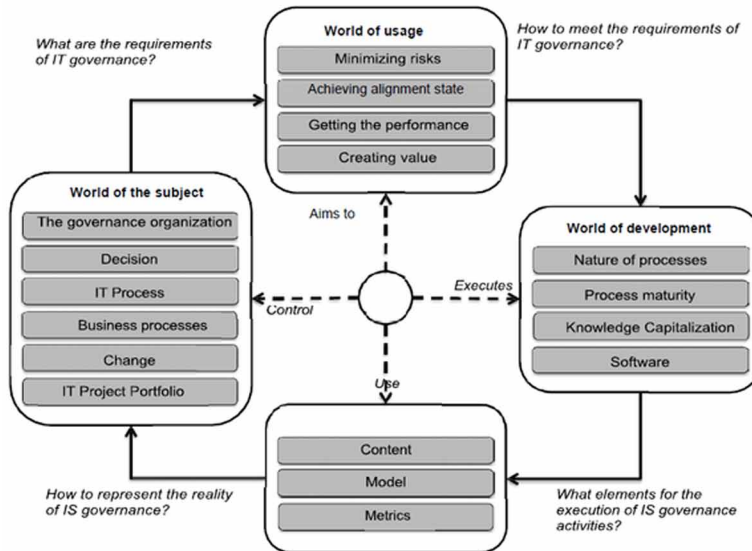
The words are in relation to each other (Claudepierre & Nurcan, 2007): The word *subject* defines a framework for identifying and justifying the purposes of the word of use. The word *system* is the support for the representation of the reality of the word subject. The word system word is built to facilitate the processes described in the word *development* word. Finally, the word system is a support for the achievement of the objectives presented in the word *use*.

The IT governance managers is thus positioned at the center of the four words: they control the governance environment and its mechanisms (subject word), sets a set of objectives to be achieved (use word), executes processes to achieve them (development word) and uses documents, models and metrics (system word).

The Word of the IT Governance Subject

The word “subject” answers the question “What is IT governance? ». It is a faceted description of the intrinsic nature of governance. This word has six facets: GOVERNANCE ORGANIZATION, DECISION, IT PROCESS,

Figure 2. Reference framework for IT governance



BUSINESS PROCESS, CHANGE and IT PROJECT PORTFOLIO. All of these facets make it possible to situate IT governance as a set of organized activities for decision-making dedicated to the choices to be made for IT project evolutions, their impacts on business processes and IT processes. Table 1 lists all the facets and their values for the subject’s word.

Table 1. List of facets of the word “subject”

Facet	Value
GOVERNANCE ORGANIZATION	Enum{centralised, decentralized, hybrid}
DECISION	Enum{IT architecture, IT infrastructure, project planification}
IT PROCESS	Enum{documented, piloted, evolutive}
BUSINESS PROCESS	Enum{productive, administrative, ad-hoc, collaborative}
CHANGE	Enum{ad-hoc, evolutive, corrective}
IT PROJECT PORTFOLIO	SET[classification mode: Enum{ monocriteria, multi-criteria} ; transformation mode: Enum{creation, maintenance, evolution}]

Organization of Governance

Weill and Ross (2004) proposes to analyze the management behaviour of information systems by comparing it to the archetypes of state governance. He thus describes the organization around decision making. Centralized decision-making responsibility is then compared to a monarchy and collaborative decision-making is compared to participatory democracy between two groups (business and IS). This decision-making structure is organized around a typology of decisions and the study shows that investment decisions in new technologies are the responsibility of the business departments, while more technical decisions concerning the architecture and infrastructure of the system are the responsibility of the IT department. (De Haes, 2005) agrees with this idea that an organization of Information systems is structured for decision-making around a committee where roles and responsibilities are distributed.

The ORGANIZATION OF GOVERNANCE facet captures this aspect. A centralized GOVERNANCE ORGANIZATION reflects a structure where responsibility for decisions is assigned to a single person. For example, the CIO can be solely responsible for IT decisions without consulting business managers. A decentralized governance structure is representative of an organization where the decision is the result of an exchange and constitutes a consensus among several stakeholders. A hybrid structure makes it possible to adopt a centralized mode of responsibility for certain types of decision and decentralized for others.

Decision

Weill and Ross (2005) propose a model structuring the decision-making process in terms of information systems governance. This study presents five types or areas of governance decisions:

- **Information Technology Principles:** These are decisions about the strategic role played by information technology
- **Architecture:** This field refers to technological choices in order to satisfy the company's organizational needs. The decision here is guided by business processes for a properly urbanized IS.
- **Infrastructure:** These are the decisions regarding the supporting technological infrastructure. It refers to the equipment and the

company's ability to implement them, or to identify outsourcing solutions depending on the criticality of strategic objectives.

- **Business Applications:** This area concerns application needs, internal developments, outsourcing, for business functionalities.

It appears that the major decisions to be made in relation to IS governance focus on the provision of IS services and on the mode of deployment of applications. Application architecture is an important decision-making aspect. This architecture could not exist without a technical support infrastructure. Finally, IS developments are ensured by a set of projects that need to be planned. The DECISION facet is described as representative of the typology of possible decisions relating to IS architecture, IS infrastructure or project planning, as shown in Table 1.

IT Process

IT governance is based on a set of processes that make it possible to control that the objectives assigned to the IS are well considered and to react if necessary. Grembergen (2004) proposes to consider the IT processes essential for IT management around a control process (reporting) and an action process for decision-making. It joins the idea developed earlier in Luftman, Papp, and Brier (1999) which advocates six steps for business/SI alignment. They mainly concern: identifying objectives, understanding alignment links, analysis (in- fine, measurement and control) and prioritization of gaps, specification and choice of actions to be taken. The IT PROCESSES are thus linked to obtaining IS quality through a control mechanism whose foundations are based on the PDCA's generic Deming approach (Plan, Do, Check, Act) (Moen, R., & Norman, 2006).

The values associated with this facet measure the degree of control of these processes based on the principle that an IT PROCESS is at least documented. The identification of metrics, indicators and control rules enables decisions to be made on the audit process: the process is then steered. An evolutionary process is a process under control whose evolution has been considered and which is representative of mature governance, as shown in Table 1.

Business Processes

Davenport (1993) defines a business process as “a structured and measured framework of activities designed to produce a specific output for a customer or market. This involves focusing on how work is done within an organization, rather than focusing on the product. A process is therefore a precise order of activities across time and space, with a clearly defined beginning and end, inputs and outputs: a structure for action. »

There are several typologies of business processes: Two approaches are used to characterize this notion (Alonso, Agrawal, El Abbadi & Mohan, 1997; Rummler & Brache, 2012). The first structure defines processes in terms of their direct/indirect contribution to value creation. The approach (Rummler, G. A., & Brache, 2012) distinguishes primary processes, which are in direct contact with the customer and directly generate value, from supporting processes.

The BUSINESS PROCESS captures these aspects. The typology of Alonso, Agrawal, El Abbadi, and Mohan (1997) is used to characterize the values of the business process facet as shown in Table 1.

Change

CHANGE management refers to the management of the organization's transformation processes and its business or IT processes. Ploesser, Recker, and Rosemann (2008) proposes a typology of change processes:

- **Change by Substitution:** The temporary replacement of one business process by another, structurally different business processes, and usually in response to an unforeseen event such as an emergency.
- **Adaptive Change:** The temporary adaptation of the structure of a business process in response to a planned and temporary event, without erasing the structural identity of the process.
- **Change by Evolution:** The changes made in the business process are permanent. They considerably modify the structural composition of the process or of its type.

The classification of Ploesser et al. (2008) is taken on the typology of business process changes and adapt it to propose the values of the change facet. Changes can be: (i) ad hoc, this is the case for unwanted changes;

(ii) evolutionary, when an improvement is envisaged; (iii) corrective, when processes are adapted to execution.

In the context of IT Governance, changes occur in business processes as well as in IT processes or IT development and maintenance projects. The CHANGE facet captures this aspect and takes its values from an enumerated domain that includes ad-hoc, evolutive and corrective values, as shown in Table 1.

IT Project Portfolio

The information system is the object of IT governance. The latter is continuously transformed to meet the support and IT services needs of the company's players. IS project portfolio management is defined as an identified practice in IT governance. Its objective is to prioritize IT transformation projects according to a set of criteria. For Reyck et al. (2005), it is a question of classifying projects according to their order of urgency in relation to these criteria. Two ways of classifying projects are identified: single-criteria or multi-criteria.

The IT PROJECT PORTFOLIO facet is complex. It makes it possible to characterize the classification mode of IT projects and the mode of IT transformation.

The Word of IT Governance Usage

The word "usage" answers the question "What are the objectives of IT governance, what is its purpose? ». It is a faceted characterization of governance objectives. This word has four facets: MINIMIZING RISKS, ATTENDING THE STATE OF ALIGNMENT, GETTING PERFORMANCE

Table 2. List of facets of the word usage

Facet	Value
MINIMIZING RISK	Enum{ extra cost, non-quality, delay }
ACHIEVING ALIGNMENT STATE	Enum{IT evolution, business evolution, co-evolution }
GETTING THE PERFORMANCE	Enum{ ad-hoc, process maturity }
CREATING VALUE	Enum{IT asset, business asset, IT usage }

and CREATING VALUE. All facets associated with this word helps to highlight the objectives of ITG. The remainder of this section provides a definition of each facet that is summarized in Table 2.

Thus, whether it is a question of managing projects, business processes or ensuring the satisfaction of IT users in terms of security, information must always be provided at the lowest cost, on time and with the expected quality.

In conclusion, the analysis and synthesis of the objectives granted to ITG lead to the following proposal shown in Table 2.

Minimizing Risks

Risk management is strongly linked to IS project portfolio management. Thus for each project it is essential to measure the impact of risks on cost, quality and deadlines. It is a question of managing projects, business processes or ensuring the satisfaction of IT users in terms of security, information must always be provided at the lowest cost, on time and with the expected quality.

The MINIMIZE RISKS facet captures the types of risks related to information needs. It takes its value in an enumerated area including extra cost, non-quality and delay as shown in Table 2.

Achieving Alignment State

The primary objective of an IS is to satisfy the need of support to the actors of an organization. The IS can also be used as a competitive advantage. The Strategic Alignment Model (SAM) developed by Henderson and Venkatraman (1999) distinguishes between the external information perspective (IT strategy) and its internal objective (IT infrastructure and process infrastructure), recognizing the potential of IT to support both the organization's business and its strategy. The model is based on two types of alignment: strategic adjustment and functional adjustment. Alignment thus consists in making business and IT strategies evolve in coherence on the one hand, and business and IT services on the other.

The facet ACHIEVING ALIGNMENT STATE takes its values on a listed domain including the values IT evolution, business evolution and co-evolution as shown in Table 2.

Getting the Performance

Performance is at the heart of the concerns of CIOs. This is the result of mastering the maturity of the business and IS processes (Ravichandran, Lertwongsatien & Lertwongsatien, 2005). In addition, the application of process-oriented methods such as COBIT or CMMi is relevant. These frameworks propose a predefined set of objectives to be achieved and metrics to measure process maturity.

Two strategies are identified for achieving governance performance: an ad-hoc strategy and a strategy guided by process maturity. This aspect is captured through the GETTING PERFORMANCE facet, which can take the ad-hoc or mature values of the processes, as shown in Table 2.

Creating Value

In the literature, two main types of value are addressed when dealing with IS. The financial value of the human, material and energy resources used (heritage value) from the value in use. Governance deals with alignment; it is therefore also relevant to analyze value creation both at IS level (IT assets) and at the organizational level (business assets). The use value (use of the IS) is linked to the efficient use of the system by its users (Grover & Kohli, 2012).

The facet CREATING VALUE captures the elements of value concerned: IT assets, business assets and IT usage.

The Word of the IT Governance System

The word of the ITG system answers the question “What information is useful for ITG activities? ». It is a faceted characterization of information media for IS governance. This word has three facets: CONTENT, MODEL and METRIC. All the facets selected to highlight the elements that are useful for IT Asset Management’s decision-making activities in terms of value creation

Table 3. List of facets of the word system

Facette	Valeur
CONTENT	Enum{document name }
MODEL	Enum{process, object, decision, evolution }
METRICS	Enum{risk, performance, value, alignment }

objectives, risk control, alignment and performance achievement. Table 3 lists all the facets and their values for the system word.

In conclusion, the analysis and synthesis of the elements of the ITG system lead to the following proposal shown in Table 3.

Content

IT governance activities are based on information media, most often documents. A document summarizes useful information for decision-making. A non-exhaustive list below is provided:

- **Documents for Alignment:** Strategic plan, IS/business process mapping;
- **Documents for Management:** Hierarchical organization chart, RACI of the members of the management committees, activity reports, description of the programs;
- **Resource Management Documents:** Incident reporting, architecture and infrastructure model;
- **Risk Management Documents:** Risk mapping, emergency plan, restoration procedure;
- **Performance Management Documents:** Dashboards;
- **Value Management Documents:** Budget, investment plan, invoices;
- **Maturity Management Documents:** Best Practices.

The CONTENT facet highlights the need for an IT governance system to manage a set of documents. It is characterized by the unique document name value as shown in Table 3.

Model

Models allow the representation of a domain and are the support for analysis and reasoning. They respect a certain paradigm, that is, a way of seeing, of representing a particular subject. ITG activities require representation of four topics:

- **Processes:** Process models are used to describe the business and IS processes. In computing, there are several languages for process modeling: the UML (Unified Modelling Language) standard (Booch, Rumbaugh & Jacobson, 1999) makes it possible to represent processes

with the activity diagram. BPMN (Business Process Modeling Notation) (Briol, 2008) is a standard maintained by the OMG (Object Management Group). It allows representing the sequence of activities, their distribution to actors, and the events inherent to a process.

- **Objects:** Object models are used to represent object classes. UML is based on object principles and provides class and object diagrams with specific notations. This paradigm is used in many computer applications including object databases, operating systems and object programming languages such as C++, C# or Java.
- **Decisions:** Decision models must allow a decision-maker to act as prescribed by certain theories of choice. In the ideal case of a totally specifiable problem, this consists in the visualization of a decision tree which makes it possible to make an optimal choice according to the desired criteria (for example minimization of risk).
- **Evolutions:** The MAP model (Rolland, 1998) was also proposed for IS and process re-engineering. It is based on the concepts of intention, which represents the projection of the need for evolution that one wishes to have for the future IS, and of the strategy that is the way to achieve these intentions.

The MODEL facet characterizes the types of models considered by a governance approach. It is based on a listed value area that contains the values: process, object, decision, and evolution. This facet reflects the ability of the governance system to represent business and IT processes, decisions, projects and their evolution.

Metric

IT governance activities are based on metrics that enable decision-makers to assess the current situation with regard to the objectives to be achieved. The metrics are thus the dimensions of “What?” measurement (the IS, its projects, processes and resources) and the “Why?” (Performance, value, risk and alignment objectives).

The METRIC facet captures this aspect and is based on a listed value domain including values: risk, performance, value and alignment.

The Word of IT Governance Development

The development word of ITG is a word that is related to the other three words of the framework. It captures the characteristics of IT governance deployment. It refers to the description of IT management processes, the way decision-making roles are distributed, the organization of the IT management committee, the way changes and innovations in the IT project portfolio are managed, the IT development processes and business processes. The development word adapts to the nature of ITG described by the subject word and its objectives described in the word of usage. ITG processes must enable performance in achieving value, risk, performance and alignment objectives. These processes are collaborative in nature for decision-making. It is therefore essential to consider how IT management actors share their knowledge and manipulate information through dedicated reporting and modeling tools. These ITG-specific processes use elements of the system word, such as the content aspects, models and metrics described in that word.

The development word is composed of four facets: **PROCESS NATURE**, **PROCESS MATURITY**, **KNOWLEDGE CAPITALIZATION** and **SOFTWARE**. All facets and their values are presented in Table 4.

In conclusion, the analysis and synthesis of the ITG development processes lead to the following proposal shown in Table 4.

Nature of Processes

A process is a set of activities that, from one or more inputs, produces one or more outcomes representing value to an internal or external client (Hammer, 1993). Referring to Hammer’s definition of processes, the IS development process is a set of activities coordinated and executed by a system engineer

Table 4. List of facets of the word development

Facette	Valeur
NATURE OF PROCESSES	Enum{ad-hoc, systematic}
PROCESS MATURITY	SET{level; Objective}
KNOWLEDGE CAPITALIZATION	Enum{socialization, externalization, internalization, combination}
SOFTWARE	Enum{ISI, CAGE}

in order to produce the governance IS. The result is a decision support and assistance system (DIS) whose use and utility must be measured.

Two approaches are distinguish to building decision support systems: (i) a collaborative approach in which the engineer progressively defines the steps of the process “on the fly”. The process is ad hoc. (ii) The development of the system can follow a set of activities known in advance. For each system creation or maintenance project, the engineer will follow predefined steps.

Process Maturity

The MATURITY level of the development process has a strong impact on the performance of ISG activities. Thus, highly mature IS management processes will generate more efficient documentation and feedback for decision making and orientation of IS management objectives and projects.

Several maturity models exist. The most proven and used by IT professionals is the CMMI (Capability Maturity Model Integrated) maintained by the Software Engineering Institute. The CMMI does not evaluate the maturity of IS management processes but that of IS development processes. However, there is a relationship with ISG because at a high level of maturity (CMMI levels 3, 4 and 5), IS processes and projects must be managed, associated with performance objectives, and must be able to evolve.

Capitalisation of Knowledge

The knowledge sharing mechanisms manipulated during ISG activities allow their CAPITALIZATION. Internalization is a process of appropriating explicit knowledge into tacit knowledge.

These aspects are captured through the KNOWLEDGE CAPITALIZATION facet defined on a domain including socialization, outsourcing, internalization and combination values.

Software

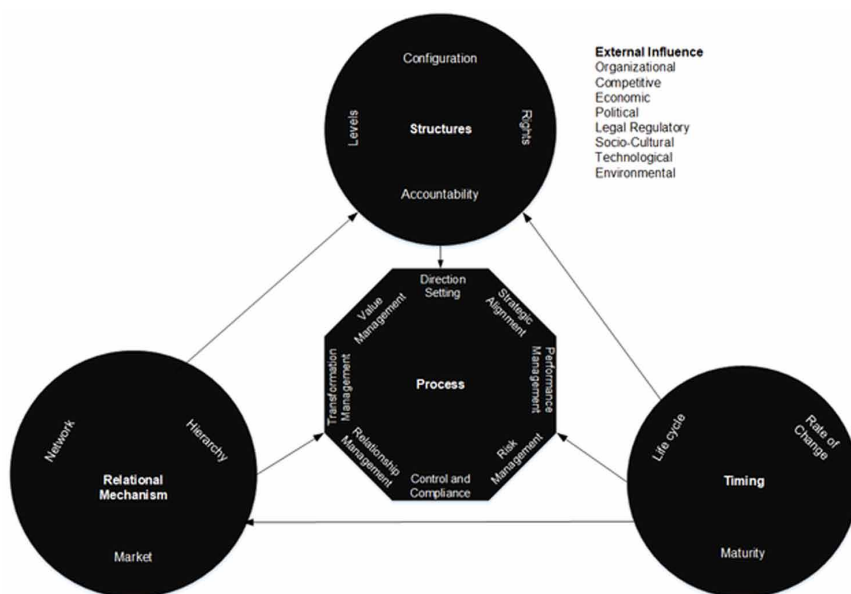
The SOFTWARE facet captures IT media dedicated to ISG. Current approaches emphasize the need to produce indicators for ISG, to present them to decision-makers in the form of dashboards. However, none deals in an integrated way with the provision of support applications to ISG. The SOFTWARE facet captures these aspects. It takes ISI (Information System Intelligence) as its

value when an approach deals with application elements dedicated to decision making for information systems. It takes as its CAGE value (Computer-aided Governance Engineering) when an approach deals with application elements to support governance engineering activities.

IT GOVERNANCE STANDARDS

Having uncovered some of the IT governance concepts and challenges, including the lack of a mutually agreed definition of IT governance, it is now useful to discuss the mechanisms that lead to realizing the anticipated benefits of IT governance. In general, IT governance can be deployed using a mixture of structures, processes, and relational mechanisms (Ali & Green, 2009; Weill & Ross, 2004). By integrating the work of Brown, Grant, and Sprott (2005a), Cadete and da Silva (2017), Grembergen (2004), Nugroho (2014), Peterson (2004), Tallon, Ramirez, and Short (2013), and Weill and Ross (2005) developed a conceptual model that describes a comprehensive view of the core elements of IT governance as depicted in Figure 3. The model is considered well matured as it covers the contingency, multidimensionality,

Figure 3. Extended IT governance model (Grant, Brown, Uruthirapathy, Mcknight, & Grant, 2007)



and dynamic nature of IT governance in addition to incorporating the major elements (structure and processes) and the four objectives (IT value delivery and strategic alignment, and performance and risk management) that drive IT governance (Nabiollahi & Sahibuddin, 2008).

Similarly, each dimension of the model (structures, processes, and relational mechanisms) consist of the necessary mechanisms for the implementation of IT governance as presented in Table 5 (Wim van Grembergen & de Haes, 2009). Even though several mechanisms exist within this model, the decision on what to implement is influenced by the context and contingencies within the organization and the interacting environment (Nfuka & Rusu, 2011).

In recent years, many organizations have undertaken a process of implementing IT governance mechanisms based on a single IT governance framework or a combination of frameworks. In general, frameworks can be categorized into groups, namely: business-oriented frameworks, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO), technology-focused frameworks (e.g., ITIL), and frameworks that aim at aligning business and technology goals (e.g., COBIT) (Warland & Ridley, 2005). Predominantly, IT governance frameworks enable executives and practitioners alike to make decisions, direct as well as evaluate and monitor governance-related activities using a common and unified approach. Adopting relevant IT governance frameworks assists executives in better understanding the critical role they play in governing IT (Marrone & Kolbe,

Table 5. The dimension of the IT governance model

Dimension	Definition
Structures	This dimension is concerned with the planning and organizational elements outlined in the high-level governance strategy of organizations. Four main governance structures are included, namely: rights, accountability, configuration, and levels.
Processes	Processes refer to the tools used for the control and evaluation of IT governance. There are eight core elements in the processes dimension, as displayed in figure 3 that organizations should enact for effective IT governance. Processes are fundamental elements of IT governance frameworks.
Relational mechanisms	Relational mechanisms refer to the internal and external relationship management required to ensure the successful implementation of IT governance. Three relational mechanisms are identified, namely: network, hierarchy, and market.
Timing	The timing dimension addresses the temporal aspects associated with IT governance implementation, namely: maturity, life cycle, and rate of change.
External influences	Different external influences shape the mix of mechanisms used by organizations and should be taken into consideration when implementing IT governance. The external influences include organizational, competitive, economic, political, legal or regulatory, socio-cultural, technological, and environmental factors.

2011). For instance, executives' commitment, strategic objectives, and resources allocation influence the adoption and selection of a particular framework (Benaroch & Chernobai, 2017; Murphy, Lyytinen, & Somers, 2018). From an evaluation perspective, many organizations use frameworks or integrate multiple governance frameworks to improve their compliance level with certain regulatory requirements (i.e., SOX), while also enhancing the internal controls environments (Nianxin Wang, Yajiong Xue, Huigang Liang, & Shilun Ge, 2011).

Some of the widespread frameworks within the IT governance sphere include COSO, ITIL, ISO 38500, and COBIT (Brown, Grant, & Sprott, 2005b). The ISO standard addresses the corporate governance of IT and is concerned with governing management processes and decision-making. On the other hand, ITIL is a framework that focuses mainly on IT service management, which enables IT departments to apply strong systematic execution of operations with stringent controls (Marrone, Gacenga, Cater-Steel, & Kolbe, 2014). COBIT is generally accepted as a standard and as a common framework for IT governance that, in comparison with COSO, provides more guidance regarding control over IT (Dahlberg & Kivijärvi, 2006; Steven De Haes, Van Grembergen, & Debreceeny, 2013; Oliver & Lainhart, 2012).

Despite their established usefulness, (Otto, 2010) suggests that IT governance frameworks cannot be simply considered as off-the-shelf solutions and they cannot be implemented without any customization due to factors such as organizational structure, business objectives, and company size. (Raghupathi, 2007) highlight an urgent need for IT governance models and frameworks that can be expanded and transformed from generic frameworks into something more relevant and applicable to businesses and organizations. In reference to the COBIT framework, (Neto, CGEIT, Assessor & de Luca Ribeiro, n.d.) states that frameworks, best practices and standards are useful only if they are adopted and adapted effectively. Accordingly, (Dahlberg & Lahdelma, 2007; Simonsson & Johnson, 2006; Webb et al., 2006) draw attention to the very little academic research that provides guidance on how to turn theories on IT governance frameworks and structures into practice.

There is no real framework that fully covers IT governance. From the point of view of standards, the information system is approached according to very different facets: production service and management (Library for Information Technology Infrastructure – ITIL), project development and organization (Integrated Maturity Level Model - CMMI, Guide to the body of knowledge - ITIL), project management (ITIL), project management (ITIL), project management (ITIL).

In project management - PMBOK), technology and process management (Information control objectives and associated technologies - CobiT and ISO 38500), security (ISO 27000).

Each standard tends to extend its field of competence, so they may end up overlapping or duplicating each other. The key is therefore integration and adaptation by choosing to build your own approach and implementing some parts of the standards rather than having the goal of implementing everything. The Cigref [28] defines the governance objectives through three questions: How are decisions made? about the information system? How to improve and gain acceptance the making of these decisions? How to ensure that these decisions will be properly made implementations? Thus, the implementation of governance must allow the ascent of understandable performance indicators, used by management to assess the proper functioning of IT services, in response to the strategic business needs (Beloglazov, Banerjee, Hartman, & Buyya, 2014). The most common IT governance standards are presented below.

COBIT

The Information Systems Audit and Control Association (ISACA) and the ITGI founded COBIT in 1992. The first edition of COBIT was published in 1996, and the fifth and latest edition was published in April 2012. The framework has grown to be, and still is, one of the most significant global frameworks for IT governance (Omari, Barnes, & Pitman, 2012). COBIT was originally built as an IT audit guideline (ISACA, 2012) because the framework contained a comprehensive set of guidelines to improve audit and compliance, provided a detailed guidance on governance practices, and offered auditors several customized checklists for various aspects of controls assessment (Hiererra, 2012). These aspects make COBIT a perfect framework for establishing control over IT and facilitating performance measurement of IT processes, as well as allowing executives to bridge the gap between control requirements, technical issues, and business risks (Brustbauer, 2016). In addition, COBIT has important business value in terms of increased compliance, corporate risk reduction, and good accountability, and is proven to be a useful tool to establish a baseline for process maturity (Nianxin Wang et al., 2011). Moreover, the framework is growing to be universally applicable due to its wide implementation as an IT governance framework (Ribeiro & Gomes, 2009; Wim van Grembergen & de Haes, 2009).

From an IT governance perspective, the main objective of COBIT is to enable value creation through ensuring benefits are realized, risk reduced, and resources optimized. It is also proclaimed to provide business stakeholders with an IT governance model that improves the management of risks associated with IT and leverages a top-down structure to ensure systematic management of the descriptive processes to achieve proper IT governance (Von Solms, 2005). The COBIT framework is considered to be a generic, comprehensive, independent, and large body of knowledge designed to measure the maturity of IT processes within organizations of all sizes, whether commercial, not-for-profit, or in the public sector (Elhasnaoui, Medromi, Chakir, & Sayouti, 2015; Nianxin Wang et al., 2011).

The COBIT framework has been steadily achieving worldwide recognition as the most effective and reliable tool for the implementation and audit of IT governance, as well as for assessing IT capability. It is regarded as the main standard to adopt for organizations striving to comply with regulations such as Sarbanes-Oxley (SOX) in the United States. It is also considered a trusted standard that has been adopted globally, as it provides extensive sets of predefined processes that can be continually revised and customized to be more effective in supporting different organizational objectives, whether for private or public industries, governments, or accounting and auditing firms (Cadete & da Silva, 2017; Guldentops, 2002; Maes, De Haes & Van Grembergen, 2013; Wim van Grembergen & de Haes, 2009; Warland & Ridley, 2005; Wood, 2010). COBIT is viewed as an exhaustive framework that encompasses a complete lifecycle of IT investment (Steven De Haes et al., 2013) and supplies IT metrics to measure the achievement of goals (Williams, Hardy, & Holgate, 2013).

It is also defined as the best framework to balance organizational IT goals, business objectives, and risks (Warland & Ridley, 2005). This is achieved by making use of (Kaplan, Kaplan, Norton & Norton, 1996) Balanced Scorecard (BSC) dimensions – Financial, Customer, Internal; and Learning and Growth – to introduce a goals cascade mechanism that translates and links stakeholders' needs to specific enterprise goals, IT-related goals, and enabler goals (COBIT processes). A set of 17 enterprise goals have been developed that are mapped to 17 IT-related goals and sequentially to the COBIT processes (ISACA, 2012a). In addition to providing a set of IT governance processes, COBIT also facilitates the appropriate implementation and effective management of these processes through establishing clear roles and responsibilities by means of a detailed Responsible, Accountable, Consulted, and Informed (RACI) matrix (Simonsson, M., Johnson, P., & Wijkström, 2007). COBIT provides

extensive sets of predefined processes which can be continuously revised and customized to be more effective in supporting different organizational objectives.

The current fifth version of COBIT is built on five basic principles: Meeting Stakeholder Needs; Covering the Enterprise End-to-End; Applying a Single, Integrated Framework; Enabling a Holistic Approach, and Separating Governance from Management. Further, the COBIT 5 Process Reference Model (PRM) divides IT into five domains:

- Evaluate, Direct and Monitor (EDM);
- Align, Plan and Organize (APO);
- Build, Acquire and Implement (BAI);
- Deliver, Service and Support (DSS); and
- Monitor, Evaluate and Assess (MEA).

The COBIT 5 domains are broken into 37 high-level IT processes and over 300 detailed IT controls covering aspects of IT management and governance (ISACA, 2012). Another distinctive feature within COBIT lies in its ability to identify seven categories of enablers (or factors) –

- Principles, policies and frameworks;
- Processes;
- Organizational structures;
- Culture, ethics and behaviour;
- Information;
- Services, infrastructure and applications;
- Availability.

Thus, it is considered the most appropriate framework to facilitate the alignment between business and IT goals (Oliver & Lainhart, 2012).

COBIT 5 transformed into a more business-oriented framework through establishing one integrated framework that consisted of different models (e.g. Val IT, Risk IT). This amalgamation was largely due to the recognized need to provide a comprehensive basis for options, not only for users and auditors but also for senior managers and business process owners in order to cover all aspects of business and functional IT responsibilities leading to effective IT governance and management outcomes. Moreover, COBIT 5 has been aligned with the ISO/IEC 15504 Process Capability Model (PCM) (ISACA, 2012). From an IT governance evaluation perspective, the shift from the

Capability Maturity Model (CMM), or the more recent Capability Maturity Model Integration (CMMI), developed by the Software Engineering Institute (SEI) to the new PCM has revolutionized COBIT, giving it a cutting edge in assessing capability at the process level instead of assessing maturity at the enterprise level (ITGI, 2007). This new approach is not only more consistent and repeatable, but is also verifiable and can demonstrate traceability against objective evidence gathered during the evaluation process (Basson, Walker, McBride, & Oakley, 2012). The PCM has been used extensively by financial institutions in Europe to conduct internal controls audits with the aim of assessing the need for improvement. This adds to the advantages organizations should expect from implementing COBIT, as the partnership between the framework and the PCM delivers a measurement scale to quantitatively evaluate the existence, adequacy, effectiveness, and compatibility of IT governance processes.

LIBRARY (ITIL)

ITIL is a framework of best practices, based on a process-based approach, with the objective to improve the delivery of high-quality IT services at a low cost. Before its creation, agencies and private sector contractors were independently creating their own IT management practices and duplicating efforts. The content of ITIL is independent of tools, vendors, or industry in which the service is executed, and can be applied to organizations of any size. However, it is not intended to be applied as-is, organizations are motivated to adapt it to meet their own business needs.

According to ITIL, service management is a set of specialized organizational capabilities for providing value to customers in the form of services. The act of transforming resources into valuable services is at the core of service management. Without these capabilities, a service organization is merely a bundle of resources that by itself has relatively low intrinsic value for customers. However, ITIL considers service management as more than just a set of capabilities. It is also a professional practice supported by an extensive body of knowledge, experience, and skills (OGC, 2008).

ITIL also defines the distinction between functions and processes. Functions are specialized organizations with certain types of work and responsible for specific outcomes. Such organizations are self-contained, with all the necessary capabilities and resources available for their performance and outcomes. For example, the Service Desk is a function of the role to be the

primary point of contact for customers when there is a service disruption. Processes, on the other hand, can be assumed as closed-loop systems, providing changes and transformations towards a specific goal and using feedback for self-reinforcing and self-corrective actions. Processes are measurable, have specific results delivered to customers, and respond to specific events. For example, the Event Management is a process responsible for monitoring all the events occurred throughout the IT infrastructure.

Up to the version 2, the ITIL focus was on processes, but since its version 3 the focus changed to business value. This change occurred as an attempt to strengthen the relationship between the organization's business needs and operational IT processes. Version 3 also recognizes the value and applicability of other standards, such as COBIT and CMMI. The current ITIL structure is composed of two components: the ITIL Core, which provides best practices applicable to organizations of all sizes and types; and the ITIL Complementary Guidance, which comprises a complementary set of publications with guidance specific to industry sectors, operating models, and technology architectures.

Structure of ITIL

The ITIL Core is composed of five publications, which provide guidelines necessary for an integrated approach for service management. These publications are discussed below:

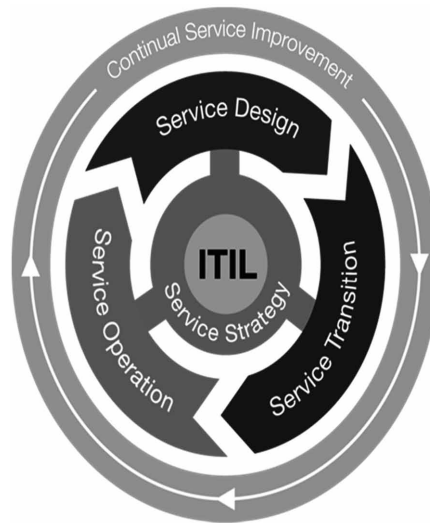
- **Service Strategy:** Provides guidance on how to view service management not only as an organizational capability but also as a strategic asset. It helps a service provider to decide on a strategy to serve customers. Starting from an evaluation of customer needs and the marketplace, the Service Strategy process determines which services the IT organization should offer and what capabilities need to develop. Its ultimate goal is to make the IT organization think and act in a strategic manner. Some topics discussed in Service Strategy are: development of service markets, characteristics of internal and external provider types, service assets, service portfolio, and implementation of strategy through the Service Lifecycle;
- **Service Design:** Has as objective to design and develop services and service management practices to be employed in the production environment. Such services should be designed with the business objectives in mind and considering the impact of changes. It is not centered only on new services, but also in the changes and improvements

necessary to increase or maintain value to customers. Among the key topics in Service Design are: service catalog, availability, capacity, continuity, and service level management;

- **Service Transition:** Helps to manage and control the changes in IT services that are implemented in the working environment of a company, in a coordinated way and ensuring their continuity. This publication provides guidance on how the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operation while controlling risks of failure and disruption. Guidance is provided while the control of services is transferred between service providers and customers. It combines practices in change, configuration, asset, release, and deployment Management.
- **Service Operation:** Embodies the practices in the management of the day-to-day operation of services to ensure they are delivered effectively and efficiently. This includes fulfilling user requests, resolving service failures, fixing problems, as well as carrying out routine operational tasks. Strategic objectives are ultimately realized through Service Operation, therefore making it a critical capability. Some topics covered by this book are: event, incident, problem, request, application, and technical management practices;
- **Continual Service Improvement (CSI):** Aims to provide guidance in creating and maintaining value for the customer through better design, transition, and operation of services. In this context, quality is a key point to achieve and maintain high levels of service provision. Thus, principles, practices, and methods from quality management, change management, and capability improvement are combined in order to learn from past successes and failures. Cost is also considered and should be consistent with the customer satisfaction. A closed-loop feedback system, based on the Plan-Do-Check-Act (PDCA) model, is established and capable of receiving inputs for improvements from any planning standpoint. Guidance on service measurement, demonstrating value with metrics, developing baselines and maturity assessments are among the key topics.

Figure 4 depicts the ITIL service management process areas and where they fit in the ITIL version 3 books. Among all the processes defined by ITIL, one of fundamental importance for this thesis, i.e., the Request Fulfillment. This process deals with service requests and it also includes the service desk functions. The service desk is the central contact point between users and IT

Figure 4. ITIL service management process areas – ITIL Core (OGC, 2008)



staff (CATER-STEEL, 2008). It is also the first place that customers contact when they have a problem or any request. If these requests and problems are not handled immediately this can cause trust issues between the customer and the service provider. Service Desk activities include managing control, communication and promotion, and providing management information.

Due to the global demands placed on IT organizations to deliver IT services, the ITIL become widely observed in the IT service industry. Diverse success cases around the world have evidenced the importance of properly managing IT infrastructures. For example, in 2000, the response time to resolve web incidents at Caterpillar was 30 minutes, but this target was not achieved until 30 minutes later. After implementing ITIL, Caterpillar has been able to hit this goal in 90% of the time. Other examples of success in implementing ITIL, include the Proctor & Gamble which saved \$125 million, according to company officials.

CMMI

The Capability Maturity Model Integration (CMMI) is a process improvement approach that provides organizations with the essential elements of effective processes. For the quality management CMMI can be used to improve the

management maturity as well as the quality of services. According to a five-level scale the processes of service provided can be systematically analyzed and the management quality improved. Originally CMMI was developed by the Software Engineering Institute from Carnegie Mellon University in 1987. This method is focused on the structured and systematic improvement of software engineering processes. During the past years, CMMI was adapted to several other business areas. The CMMI model describes five levels of process maturity. On the first level (initial) there are processes defined. On the second level (repeatable) several tasks for a process management are implemented and processes can be managed with repeatable levels of performance. In the third level (defined), processes are defined and documented within the organization. The level four (managed) focuses on the quality and performance measurement of the existing processes. Level five (optimized) demands the implementation of continuous improvement programs in the organization for optimizing quality and performance of processes.

The software process improvement capability determination (SPICE) method was originally developed for managing the software development processes. The SPICE approach is also a maturity management method which supports the quality and performance of implemented services in an organization. The SPICE method is a two-dimensional approach for managing development processes. The first dimension consists of the processes that are actually assessed (the process dimension which is grouped into five categories). The second dimension consists of the capability scale that is used to evaluate the process capability (the capability dimension). The same capability scale is used across all processes (El Emam & Birk, 2000). The ISO/IEC 15504 is an international standard on software process assessment. It defines a number of software engineering processes, and a scale for measuring their capability. In ISO/IEC 15504, there are 5 levels of capability that can be rated, from Level 1 to Level 5. The rating scheme consists of a 4-point achievement scale for each attribute. The four points are designated as F, L, P, N for Fully Achieved, Largely Achieved, Partially Achieved, and Not Achieved (El Emam & Birk, 2000).

CMMI is a quality approach for software development that allows better allocation of resources, better management and thus a reduction in costs and a reduction in the superior timeliness. The approach is integrated into the transformation of IS to supervise the development of its developments.

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

The Committee of Sponsoring Organizations of the Treadway Commission (commonly referred to as COSO) was convened by the U.S. Congress in response to well-publicized financial irregularities that occurred in the late 1980s. COSO formulated an internal control framework designed to help organizations reduce the risk of asset loss, ensure the reliability of financial statements and compliance with laws and regulations, and promote efficiency. COSO is recognized by many public sectors and professional bodies as a standard for the evaluation of internal control and the risk environment. Under the COSO framework, the effectiveness of an internal control system is measured by its capacity to provide reasonable assurance to management and to the board of directors of their bank's achievement of its objectives in three categories:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting,
- Compliance with applicable laws and regulation.

The emphasis on behavior in the COSO model is a recognition of reality, namely that policies specify what management wants to happen; what actually happens, and which rules are obeyed, bent, or ignored, is determined by corporate culture. The COSO internal control model consists of five interrelated components, which are inherent in the way management runs the organization. The components are linked, and serve as criteria for determining whether or not the system is effective. The COSO components include control environment, risk assessment, control activities, monitoring and learning, and information and communication. The COSO enterprise risk management framework and key components of operational risk approach.

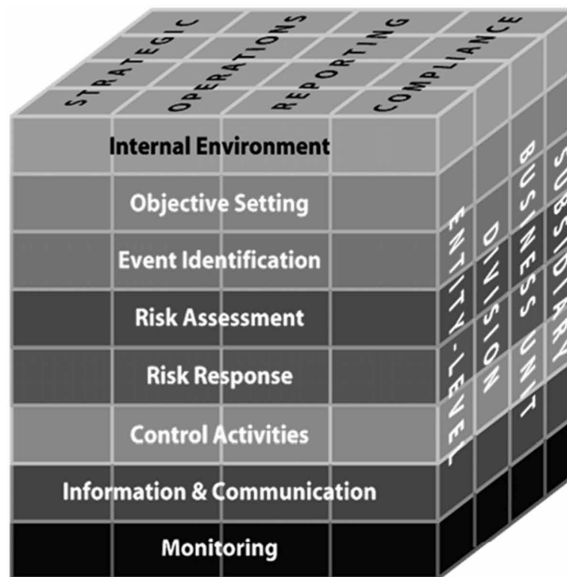
Another important theme addressed by COSO is the enterprise risk management. COSO divides the enterprise risk management (ERM) framework into eight interrelated components as shown in Figure 5, including the following:

- **Internal Environment:** Internal environment describes the work environment and risk preferences of an organization and sets the framework for how risk is viewed and addressed by its management

and employees. Internal environment includes risk management philosophy, risk appetite, integrity and ethical values, and the environment in which they operate.

- **Objective Setting:** Objectives must be set up-front. Risk management function should ensure that there is a process for corporate management to set the objectives, that the chosen objectives support and align with the entity’s mission, and that they are consistent with its risk appetite.
- **Event Identification:** Internal and external events affecting the achievement of an entity’s objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management’s strategy or objective-setting processes.
- **Risk Assessment:** Risks are analyzed, considering the likelihood of occurrence and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- **Risk Response:** Management selects risk responses—avoiding, accepting, reducing, or sharing risk—developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.
- **Control Activities:** Policies and procedures should be established and implemented to help ensure the risk responses are effectively carried out.

Figure 5. The ERM Model proposed by COSO



- **Information and Communication:** Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense—flowing down, across, and up the entity.
- **Monitoring:** The entirety of enterprise risk management must be monitored and modifications made as necessary.

PMBOOK

Project Management Body of Knowledge (PMBOK), whose origins date back to 1983 with a first publication by the global non-profit organization Project Management Institute (PMI) aims to standardize project management approach and procedures. The first PMBOK was published in 1996 and recognized as an official ANSI standard since 1999. This standard has very strong support; in 2015 there were 476,000 members in 204 countries. PMBOK defines a set of 47 processes grouped around these 5 parent processes: 1 - Start-up, 2- Planning, 3 - Execution, 4 - Monitoring and Control, 5 - Closing. Each process details input transformation mechanisms (planning, design documents) into outputs (documents, products. .)[29]. PMBOK is complementary to the CMMI continuous improvement approach.

ISO/IEC 27001:2005 (Revised by ISO/IEC 27001:2013)

ISO 27000 is a suite of good practices grouped into standards that deal with information security. Written from 2005, it is constantly evolving. The ISO 27000 version published in 2009 is a short 38-page introductory document defining the family of standards and terms. The only standard leading to certification is ISO 27001, which defines a set of requirements and control points to protect IT assets against any loss, theft, intrusion or alteration of the IT system. ISO 207002 is a good practice guide listing measures for implementing or maintaining an Information Security Management System (ISMS) (ISO, 2013). Good practices are applied IS security rules to guarantee the protection of its infrastructure.

The international standard is not tailored to any specific industry, thus, a wide range of organizations may seek certification of their Information Security Management System (ISMS). Over 7,300 organizations worldwide have already been certified compliant with ISO/IEC 27001 or equivalent

national variants. Even though certification is not compulsory, it is increasingly being demanded by some business partnerships. In terms of marketing, the certificate gives assurance to business partners of the status of the organization with regards to information security without the necessity of conducting their own security reviews. Getting certified under ISO/IEC 27001 is a means of providing assurance that the organization has not only implemented a system for the management of information security, but also maintains and continuously improves the system. Suitable uses of the standard include the following (ISO, 2013):

- Use within organizations to formulate security requirements and objectives;
- Use within organizations as a way to ensure that security risks are cost-effectively managed;
- Use within organizations to ensure compliance with laws and regulations;
- Use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met;
- Definition of new information security management processes;
- Identification and clarification of existing information security management processes;
- Use by the management of organizations to determine the status of information security management activities;
- Use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization;
- Use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons;
- Implementation of business-enabling information security;
- Use by organizations to provide relevant information about information security to customers.

Structure of ISO/IEC 27001:2005

The 34-page document is structured into nine sections and has three appendices. The highlight of each section is described below:

- **Introduction:** Asserts the standard uses a process approach.
- **Scope:** It specifies generic ISMS requirements suitable for organizations of any type, size or nature.
- **Normative References:** The standard recommends the essential use of ISO/IEC 27002:2005
- **Terms and Definitions:** A brief, formalized glossary
- **Information Security Management System:** The details of the standard, based on the Plan-Do-Check-Act cycle where Plan = define requirements, assess risks, decide which controls are applicable; Do = implement and operate the ISMS; Check = monitor and review the ISMS; Act = maintain and continuously improve the ISMS. Also specifies certain specific documents that are required and must be controlled, and states that records must be generated and controlled to prove the operation of the ISMS (e.g. certification audit purposes).
- **Management Responsibility:** Management must demonstrate their commitment to the ISMS, principally by allocating adequate resources to implement and operate it.
- **Internal ISMS Audits:** The organization must conduct periodic internal audits to ensure the ISMS incorporates adequate controls which operate effectively.
- **Management Review of the ISMS:** Management must review the suitability, adequacy and effectiveness of the ISMS at least once a year, assessing opportunities for improvement and the need for changes.
- **ISMS Improvements:** The organization must continually improve the ISMS by assessing and where necessary making changes to ensure its suitability and effectiveness, addressing nonconformance (noncompliance) and where possible preventing recurrent issues.
- **Annex A:** Control objectives and controls - little more in fact than a list of titles of the control sections in ISO/IEC 27002, down to the second level of numbering (e.g. 9.1, 9.2), 133 in total.
- **Annex B:** OECD principles and this International Standard - a table briefly showing which parts of this standard satisfy 7 key principles laid out in the OECD Guidelines for the Security of Information Systems and Networks.
- **Annex C:** Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard - the standard shares the same basic structure of other management systems standards, meaning that an organization which implements any one should be familiar with concepts such as PDCA, records and audits.

ISO/IEC 27002:2005 (Revised by ISO/IEC 27002:2013)

ISO/IEC 27002:2005 is another generic standard that can be applied to health information systems to ensure security. It establishes general principles and guidelines for effective initialization, implementation, maintenance and improvement of information security management. The objectives outlined therein provide general guidance on the commonly accepted goals of information security management. Thus any organization seeking to adopt a comprehensive information security management program or improve its existing information security practices can use the standard. The ISO standard asserts that information can be protected using a wide variety of controls. Such controls include hardware and software functions, procedures, policies, processes and organizational structures. Organizations including healthcare organizations, must develop, implement, monitor, evaluate and improve these types of security controls. (PRGL, 2011).

COMPARISON AND ANALYSIS

The six different governance approaches reviewed each cover specific IS properties. IS governance is a large-scale project that requires prior evaluation in order to avoid failure during its implementation.

IT governance concerns mid-sized and larger companies. Initiating and undertaking governance work is complex, time-consuming and costly. It requires ongoing stakeholder investment and the establishment of teams to implement the governance project. The cost of implementation can be significant: training of the persons concerned in the company; use of an external consultant; certification of the standard. Governance does not solve all problems, as we have seen, each of the approaches is dedicated to specific subjects. Because of its implementation cost, a return on investment is even less guaranteed.

Governance specifically concerns the discipline of management information technology. This thesis is concerned with the alignment between trades and software architectures. One of the subjects of governance would seem to be able to respond to our concern, indeed, governance addresses the notion of alignment. Table 6 compares the different IT governance standards (CobiT, COSO, ITIL, CMMI, PMBOK) according to the four words described in section 2.

A Deep Overview of Information Technology Governance Standards

Table 6. IT governance standards and models comparison according to the four words

The frame of the Four Words	Facet	IT Governance Standards and Models				
		CobIT	COSO	ITIL	CMMI	PMBOK
<i>Subject</i>	GOVERNANCE ORGANIZATION	*	*	-	-	*
	DECISION	-	-	<i>Infrastructure</i>	-	<i>Plan, project</i>
	IT PROCESS	*	*	*	*	*
	BUSINESS PROCESS	-	*	*	-	*
	CHANGE	*	-	<i>Evolutive</i>	*	*
<i>Usage</i>	IT PROJECT PORTFOLIO	-	-	*	<i>Clas.: Multi-criteria Transfo.: *</i>	<i>Clas.: Multi-criteria Transfo.: *</i>
	MINIMIZE RISKS	*	*	<i>quality</i>	*	*
	REACH ALIGNMENT STATUS	-	-	<i>IT Evolution</i>	-	<i>IT Evolution, Business evolution</i>
	GETTING PERFORMANCE	-	-	-	<i>Process Maturity</i>	<i>Process Maturity</i>
	CREATE VALUE	-	<i>Business Asset</i>	<i>IT Asset, usage</i>	<i>IT Asset</i>	<i>IT Asset, Business Asset</i>
<i>System</i>	CONTENT	<i>document</i>	<i>document</i>	<i>document</i>	<i>document</i>	<i>document</i>
	MODELE	<i>Process, object</i>	<i>Process, object</i>	<i>Process, objet</i>	<i>Process, object</i>	<i>Process, object, decision</i>
	METRICS	<i>Risk, performance, value</i>	<i>Risk</i>	<i>Alignment, performance</i>	<i>Performance</i>	<i>Risk, Performance, Value</i>
<i>Development</i>	NATURE	systematic	systematic	systematic	systematic	systematic
	DES PROCESSUS					
	PROCESS MATURITY	*	-	-	*	*
	CAPITALISATION DE LA CONNAISSANCE	<i>externalization</i>	<i>externalization</i>	<i>externalization</i>	<i>externalization</i>	<i>externalization</i>
	SOFTWARE	*	*	*	*	*

*Fully covered facet, - Uncovered facet

This overview of the main IT governance methods has enabled us to understand more fully what governance means and the role of each of them: security, quality, supply, services, standardization, project management and costs. The application of different good governance practices influences the operational aspects of IT transformation and facilitates its management and control. Knowing the governance function for the IT also means avoiding

confusing it with the enterprise architecture, which is also concerned with the IT.

Most IT governance frameworks are designed to help you determine how your IT department is functioning overall, what key metrics management needs and what return IT is giving back to the business from its investments.

Where COBIT and COSO are used mainly for risk, ITIL helps to streamline service and operations. Although CMMI was originally intended for software engineering, it now involves processes in hardware development, service delivery and purchasing. As previously mentioned, FAIR is squarely for assessing operational and cybersecurity risks.

Though COBIT is one of the most popular frameworks used by publicly traded companies in the US to comply with the Sarbanes-Oxley Act, the purpose is for IT management and compliance. It helps to strengthen the security of healthcare systems, but security is not the main goal of COBIT. This standard may not be suitable for small healthcare organizations who want to improve the security of their system.

ISO/IEC 27002:2005 can be applied to the organization of any size concerned with the information security of their systems. An organization can use this standard as a guide to managing their information security program. Organizations can seek certification for their Information Security Management System to be compliant with ISO/IEC 270001: 2005.

When reviewing frameworks, consider your corporate culture. Does a particular framework or model seem like a natural fit for your organization? Does it resonate with your stakeholders? That framework is probably the best choice. However, you don't have to choose only one framework. For example, COBIT and ITIL complement one another in that COBIT often explains why something is done or needed where ITIL provides the "how." Some organizations have used COBIT and COSO, along with the ISO 27001 standard (for managing information security).

CONCLUSION

This chapter proposed a faceted framework for the analysis of IT governance. This framework considers four perspectives, called words of the subject, use, system and development of ITG. Facets and their values detail these four perspectives. This framework has been applied to 5 known IT governance standards. This application exercise revealed that none of the current approaches covers all facets of the framework. The approaches do not have an overall

vision of ITG but piecemeal visions. The emphasis is on collections of good practices that are updated regularly. This work on the state of the art has highlighted the need for research on the globality of ITG. The aim of this chapter was to provide a comprehensive understanding of ITG.

The next chapter will discuss the practices of organizations in terms of IT governance. It will present an evaluation of ITG through a case study in the Middle East and North African Large Organizations.

REFERENCES

- Aasi, P., Rusu, L., & Han, S. (2014). Culture Influence on IT Governance: What We Have Learned? *International Journal of IT/Business Alignment and Governance*, 5(1), 34–49. doi:10.4018/ijitbag.2014010103
- Al Omari, L., Barnes, P. H., & Pitman, G. (2012). An exploratory study into audit challenges in IT governance : a Delphi approach. In *Symposium on IT Governance, Management and Audit*. University of Tenaga Nasional. Retrieved from <https://eprints.qut.edu.au/53110/>
- Ali, S., & Green, P. (2009). IT governance mechanisms in public sector organisations: An Australian context. *Handbook of Research on Information Management and the Global Landscape*, 458–478.
- Alonso, G., Agrawal, D., El Abbadi, A., & Mohan, C. (1997). Functionality and limitations of current workflow management systems. *IEEE Expert*, 12(5), 105–111.
- Basson, G., Walker, A., McBride, T., & Oakley, R. (2012). ISO/IEC 15504 measurement applied to COBIT process maturity. *Benchmarking: An International Journal*, 19(2), 159–176. doi:10.1108/14635771211224518
- Beloglazov, A., Banerjee, D., Hartman, A., & Buyya, R. (2014). Improving Productivity in Design and Development of Information Technology (IT) Service Delivery Simulation Models. *Journal of Service Research*, 18(1), 75–89. doi:10.1177/1094670514541002
- Benaroch, M., & Chernobai, A. (2017). Operational IT Failures, IT Value Destruction, and Board-Level IT Governance Changes. *Management Information Systems Quarterly*, 41(3), 729–762. doi:10.25300/MISQ/2017/41.3.04

- Booch, G., Rumbaugh, J., & Jacobson, I. (1999). *The unified modeling language user guide*. Academic Press.
- Briol, P. (2008). *BPMN, the Business Process Modeling Notation Pocket Handbook*. LuLu. Com.
- Brown, A. E., Grant, G. G., & Sprott, E. (2005a). Framing the Frameworks: A Review of It Governance Research. *Communications of the Association for Information Systems*, 15(May), 696–712.
- Brown, A. E., Grant, G. G., & Sprott, E. (2005b). Framing the Frameworks: A Review of It Governance Research. *Communications of the Association for Information Systems*, 15, 696–712.
- Brustbauer, J. (2016). Enterprise risk management in SMEs: Towards a structural model. *International Small Business Journal*, 34(1), 70–85. doi:10.1177/0266242614542853
- Cadete, G. R., & da Silva, M. M. (2017). *Assessing IT Governance Processes Using a COBIT5 Model BT - Information Systems*. Cham: Springer International Publishing.
- Claudepierre, B., & Nurcan, S. (2007). A framework for analysing IT governance approaches. *ICEIS 2007 - 9th International Conference on Enterprise Information Systems, Proceedings*, 512–516. Retrieved from <http://www.scopus.com/inward/record.url?eid=2-s2.0-70349560477&partnerID=40&md5=2b2b4447a92d4202094243103e916a44>
- Dahlberg, T., & Kivijärvi, H. (2006). An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument. *39th Hawaii International Conference on System Sciences*, 0(C), 1–10. 10.1109/HICSS.2006.57
- Dahlberg, T., & Lahdelma, P. (2007). IT governance maturity and IT outsourcing degree: An exploratory study. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. 10.1109/HICSS.2007.306
- Davenport, T. H. (1993). *Process innovation: reengineering work through information technology*. Harvard Business Press.

De Haes, S., & Van Grembergen, W. (2005). IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 237b–237b. 10.1109/HICSS.2005.362

De Haes, S., Van Grembergen, W., & Debreceeny, R. S. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems*, 27(1), 307–324. doi:10.2308/isys-50422

De Reyck, B., Grushka-Cockayne, Y., Lockett, M., Calderini, S. R., Moura, M., & Sloper, A. (2005). The impact of project portfolio management on information technology projects. *International Journal of Project Management*, 23(7), 524–537. doi:10.1016/j.ijproman.2005.02.003

El-Mekawy, M., Rusu, L., & Perjons, E. (2015). An evaluation framework for comparing business-IT alignment models: A tool for supporting collaborative learning in organizations. *Computers in Human Behavior*, 51, 1229–1247. doi:10.1016/j.chb.2014.12.016

Elhasnaoui, S., Medromi, H., Chakir, A., & Sayouti, A. (2015). A new IT Governance architecture based on multi agents system to support project management. *2015 International Conference on Electrical and Information Technologies (ICEIT)*, 43–46. 10.1109/EITech.2015.7162957

Grant, G., Brown, A., Uruthirapathy, A., Mcknight, S., & Grant, G. G. (2007). Association for Information Systems AIS Electronic Library (AISeL) An Extended Model of IT Governance: A Conceptual Proposal. *AMCIS 2007 Proceedings*, 215. Retrieved from <http://aisel.aisnet.org/amcis2007%0Ahttp://aisel.aisnet.org/amcis2007/215>

Grembergen, W. V. (2004). *Strategies for information technology governance*. IGI Global. doi:10.4018/978-1-59140-140-7

Grover, V., & Kohli, R. (2012). Cocreating IT value: New capabilities and metrics for multifirm environments. *Management Information Systems Quarterly*, 36(1), 225–232.

Grunwel, D., & Sahama, T. (2016). Delegation of access in an information accountability framework for eHealth. *Proceedings of the Australasian Computer Science Week Multiconference on - ACSW '16*, 1–8. 10.1145/2843043.2843383

- Guldentops, E. (2002). Governing Information Technology Through CobiT BT. *Integrity, Internal Control and Security in Information Systems: Connecting Governance and Technology*, 115–159. doi:10.1007/978-0-387-35583-2_8
- Guldentops, E., Van Grembergen, W., & De Haes, S. (2002). Control and governance maturity survey: Establishing a reference benchmark and a self assessment tool. *Information Systems Control Journal*, 6, 32–35.
- Henderson, J. C., & Venkatraman, H. (1999). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, 32(1), 472–484. doi:10.1147/j.382.0472
- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154–165. doi:10.1016/j.dss.2009.02.005
- Hiererra, S. E. (2012). *Assessment of IT Governance Using COBIT 4.1 Framework Methodology: Case Study University IS Development in IT Directorate* (Masters Thesis). BINUS University, Jakarta, Indonesia.
- Information Security Governance: Guidance for Boards of Directors and Executive Management Guidance for Boards of Directors and Executive Management. (2006). IT Governance Institute.
- ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL: Information Systems Audit and Control Association.
- ISO. (2013). *ISO Home: Standards*. Retrieved March 24, 2013 from ISO Website: [Http://www.iso.org/iso/home/standards.htm](http://www.iso.org/iso/home/standards.htm)
- ITGI. (2007). *COBIT Mapping Overview of International IT Guidance* (2nd ed.). Rolling Meadows, IL: IT Governance Institute.
- Jarke, M., Mylopoulos, J., Schmidt, J. W., & Vassiliou, Y. (1992). DAIDA: An environment for evolving information systems. *ACM Transactions on Information Systems*, 10(1), 1–50. doi:10.1145/128756.128757
- Jarke, M., & Pohl, K. (1993). Establishing visions in context: towards a model of requirements processes. *International Conference on Information Systems (ICIS)*, 23–24.
- Kaplan, R. S., Kaplan, R. S., Norton, D. P., & Norton, D. P. (1996). *The balanced scorecard: translating strategy into action*. Harvard Business Press.

Luftman, J., Papp, R., & Brier, T. (1999). Enablers and Inhibitors of business-IT Alignment. *Commun. AIS*, 1(3es). Retrieved from <http://dl.acm.org/citation.cfm?id=374122.374123>

Maes, K., De Haes, S., & Van Grembergen, W. (2013). Investigating a Process Approach on Business Cases: An Exploratory Case Study at Barco. *International Journal of IT/Business Alignment and Governance*, 4(2), 37–53. doi:10.4018/ijitbag.2013070103

Maleh, Y., Zaydi, M., Sahid, A., & Ezzati, A. (2018). Building a Maturity Framework for Information Security Governance Through an Empirical Study in Organizations. In Y. Maleh (Ed.), *Security and Privacy Management, Techniques, and Protocols* (pp. 96–127). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-5583-4.ch004

Marrone, M., Gacenga, F., Cater-Steel, A., & Kolbe, L. (2014). IT service management: A cross-national study of ITIL adoption. *Communications of the Association for Information Systems*, 34(1), 865–892.

Marrone, M., & Kolbe, L. M. (2011). Uncovering ITIL claims: IT executives' perception on benefits and Business-IT alignment. *Information Systems and e-Business Management*, 9(3), 363–380. doi:10.1007/10257-010-0131-7

McKay, J., Marshall, P., & Smith, L. (2003). Steps Towards Effective IT Governance: Strategic IT Planning, Evaluation and Benefits Management. *Pacific Asia Conference on Information Systems*, 956–970. Retrieved from <http://www.pacis-net.org/file/2003/papers/is-strategy/214.pdf>

Moen, R., & Norman, C. (2006). *Evolution of the PDCA cycle*. Academic Press.

Murphy, K., Lyytinen, K., & Somers, T. (2018). A Socio-Technical Model for Project-Based Executive IT Governance. *Proceedings of the 51st Hawaii International Conference on System Sciences | 2018 A*, 9, 4825–4834.

Nabiollahi, A., & Sahibuddin, S. (2008). Considering service strategy in ITIL V3 as a framework for IT Governance. In *2008 International Symposium on Information Technology (Vol. 1)*, pp. 1–6. Academic Press. 10.1109/ITSIM.2008.4631631

Nehan, Y. R., & Deneckere, R. (2007). Component-based situational methods: A framework for understanding SME. *IFIP International Federation for Information Processing*, 244, 161–175. doi:10.1007/978-0-387-73947-2_14

- Neto, J. S., & de Luca Ribeiro, C. H. (n.d.). Is COBIT 5 Process Implementation a Wicked Problem? *COBIT Focus*, 2, 8–10.
- Nfuka, E. N., & Rusu, L. (2011). The effect of critical success factors on IT governance performance. *Industrial Management & Data Systems*, 111(9), 1418–1448. doi:10.1108/02635571111182773
- Nugroho, H. (2014). Conceptual model of IT governance for higher education based on COBIT 5 framework. *Journal of Theoretical and Applied Information Technology*, 60(2), 216–221.
- Nurcan, S., & Rolland, C. (2003). A multi-method for defining the organizational change. *Information and Software Technology*, 45(2), 61–82. doi:10.1016/S0950-5849(02)00162-3
- Oliver, D., & Lainhart, J. (2012). COBIT 5: Adding Value Through Effective Geit. *EDPACS*, 46(3), 1–12. doi:10.1080/07366981.2012.706472
- Otto, B. (2010). IT Governance and Organizational Transformation: Findings From an Action Research Study. *AMCIS*, 421.
- Peterson, R. (2004). Crafting information technology governance. *Information Systems Management*, 21(4), 7–22. doi:10.1201/1078/44705.21.4.20040901/84183.2
- Peterson, R., Parker, M., Ribbers, P., Peterson, R. R., & Parker, M. M. (2002). Information Technology Governance Processes Under Environmental Dynamism: Investigating Competing Theories of Decision Making and Knowledge Sharing. *ICIS 2002 Proceedings*, 562–575.
- Ploesser, K., Recker, J., & Rosemann, M. (2008). Towards a Classification and Lifecycle of Business Process Change A Classification and Lifecycle of Process Change Strategies. *BPMDs'08: Business Process Life-Cycle: Design, Deployment, Operation & Evaluation*, 2008, 10–18.
- Prieto-Diaz, R. (1991). Implementing Faceted Classification for Software Reuse. *Communications of the ACM*, 34(5), 88–97. doi:10.1145/103167.103176
- Raghupathi, W. (2007). Corporate Governance of IT: A Framework for Development. *Communications of the ACM*, 50(8), 94–99. doi:10.1145/1278201.1278212

Ravichandran, T., Lertwongsatien, C., & Lertwongsatien, C. (2005). Effect of Information Systems Resources and Capabilities on Firm Performance: A Resource-Based Perspective. *Journal of Management Information Systems*, 21(4), 237–276. doi:10.1080/07421222.2005.11045820

Reich, B. H., & Benbasat, I. (2000). Factors That Influence the Social Dimension of Alignment between Business and Information Technology Objectives. *Management Information Systems Quarterly*, 24(1), 81–113. doi:10.2307/3250980

Ribeiro, J., & Gomes, R. (2009). IT Governance using COBIT implemented in a High Public Educational Institution – A Case Study. *Proceedings of the 3rd International Conference on European Computing Conference*, 41–52. Retrieved from wseas.us/e-library/conferences/2009/georgia/CCI/CCI04.pdf

Rolland, C. (1998). A comprehensive view of process engineering. *International Conference on Advanced Information Systems Engineering*, 1–24.

Rummler, G. A., & Brache, A. P. (2012). *Improving performance: How to manage the white space on the organization chart*. John Wiley & Sons.

Simonsson, M., & Johnson, P. (2006). Assessment of IT Governance - A Prioritization of Cobit. *Proceedings of the Conference on Systems Engineering Research*. Retrieved from <http://sse.stevens.edu/fileadmin/cser/2006/papers/151-Simonsson-Assessment of IT Governance.pdf>

Simonsson, M., Johnson, P., & Wijkström, H. (2007). Model-based IT governance maturity assessments with COBIT. *ECIS*, 1276–1287.

Smits, D., & Hillegersberg, J. V. (2015). IT Governance Maturity: Developing a Maturity Model Using the Delphi Method. In *2015 48th Hawaii International Conference on System Sciences* (pp. 4534–4543). Academic Press. 10.1109/HICSS.2015.541

Tallon, P. P., Ramirez, R. V., & Short, J. E. (2013). The Information Artifact in IT Governance: Toward a Theory of Information Governance. *Journal of Management Information Systems*, 30(3), 141–178. doi:10.2753/MIS0742-1222300306

van Grembergen, W., & de Haes, S. (2009). *COBIT as a Framework for Enterprise Governance of IT BT - Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value*. Boston, MA: Springer US; doi:10.1007/978-0-387-84882-2_5

- Vlietland, J., van Solingen, R., & van Vliet, H. (2016). Aligning codependent Scrum teams to enable fast business value delivery: A governance framework and set of intervention actions. *Journal of Systems and Software, 113*, 418–429. doi:10.1016/j.jss.2015.11.010
- Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security, 24*(2), 99–104. doi:10.1016/j.cose.2005.02.002
- Wang, Xue, Liang, & Ge. (2011). The Road to Business-IT Alignment: A Case Study of Two Chinese Companies. *Communications of AIS, 2011*(28), 415–436.
- Warland, C., & Ridley, G. (2005). Awareness of IT Control Frameworks in an Australian State Government: A Qualitative Case Study. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 0*(C), 236b–236b. 10.1109/HICSS.2005.116
- Webb, P., Pollard, C., & Ridley, G. (2006). Attempting to define IT governance: Wisdom or folly? *Proceedings of the Annual Hawaii International Conference on System Sciences, 8*(C), 1–10. 10.1109/HICSS.2006.68
- Weber, L. (2014). *Addressing the incremental risks associated with adopting a Bring Your Own Device program by using the COBIT 5 framework to identify keycontrols* (Doctoral Dissertation). Stellenbosch University.
- Weill, P., & Ross, J. (2005). A Matrixed Approach to Designing IT Governance. *MIT Sloan Management Review, 46*(2), 26–34. doi:10.1177/0275074007310556
- Weill, P., & Ross, J. W. (2004). *How Top Performers Manage IT Decisions Rights for Superior Results*. In *IT Governance* (pp. 1–10). Harvard Business School Press. doi:10.2139/ssrn.664612
- Williams, S. P., Hardy, C. A., & Holgate, J. A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electronic Markets, 23*(4), 341–354. doi:10.1007/12525-013-0137-3
- Wood, D. J. (2010). *Assessing IT Governance Maturity: The Case of San Marcos, Texas* (Masters Thesis). Texas State University, San Marcos, TX.

Section 2

Evaluating Information Technology in Large Organizations

Chapter 3

Evaluation of IT Governance in Middle East and North African Large Organizations

ABSTRACT

This chapter provides a deeper understanding of IT governance frameworks and their adoption, drawing on established information systems theories. A mixed two-stage approach using quantitative and qualitative studies is used to examine the feasibility of developing an IT governance assessment framework based on COBIT to assess IT governance in a specific context. The first step seeks to identify key COBIT best practices within organizations. A survey of 20 large organizations in the MENA region was adopted. In the second phase, a case study used to explore the factors that influence the adoption of the adapted IT governance assessment framework.

INTRODUCTION

Strategic Information technology IT has become an indispensable element for success in the contemporary business world as the dependency on IT by many organizations today to support, sustain and drive organizational growth increases (Shaun Posthumus & von Solms, 2004). Business and IT (information technology) alignment are considered one of the main issues in the management of the company's IS (information system). However, alignment is described as an object that can never be completely achieved

DOI: 10.4018/978-1-5225-7826-0.ch003

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

and must be adjusted frequently within the organization (Baker & Jones, 2008). To maximize alignment facilitators and minimize inhibitors, various frameworks are developed for IT Governance (ITG), which is an important concept for IT organizations in enterprises (Joshi, Bollen, Hassink, De Haes, & Van Grembergen, 2018).

Many professionals and researchers believe that Information System Governance is a complex subject. The words that immediately come to mind are “Arid, Boring, Wave, Unrealistic”. This is mainly due to the intensive use of jargon such as “strategic alignment, organizational transformation, value creation, synergy creation”, complicated vision and mission statements, which the average person finds difficult to understand (Peterson, 2001). The result is that IT governance is as poorly adopted as corporate governance because of the lack of understanding of its role within an organization (Turel & Bart, 2014).

The purpose of this chapter is to determine how to effectively adopt frameworks, best practices and standards as organizations face significant challenges in meeting their IT governance obligations. Despite the potentially costly consequences of IT and business alignment failure, there is little direct guidance to organizations on how to provide, demonstrate and maintain adequate IT governance (Renaud, Walsh, & Kalika, 2016).

A key aspect of this problem is twofold. The finding is that there is a lack of theoretical knowledge on examining the adoption and adaptation of IT governance frameworks. Although the topic of IT governance has gained popularity, there is little academic research on the subject (Marrone & Kolbe, 2011). On the other hand, IT governance concerns are very present in professional journals and reports, which advocate the need to deploy frameworks and standards to address governance challenges. Thus, several different models and standards have been developed for IT governance, of which COBIT is most often used. Research shows that efforts devoted to these models and standards can help create value, improve productivity, optimize resources, increase compliance, reduce costs and improve lead times (Beloglazov, Banerjee, Hartman, & Buyya, 2014).

The adoption of best practice frameworks by IT departments is aimed at providing IT services to business entities more effectively and efficiently according to their demand. When IT begins its journey to better support business, a chain of events will begin that requires adopting standards and best practices that meet business service needs (Ryan Peterson, Parker, Ribbers,

Peterson, & Parker, 2002). Furthermore, it takes significant time to fully implement a framework the size of COBIT in its entirety. Such timeframes mean that the COBIT framework is often considered an expensive approach for many organizations, as significant resources need to be allocated over an extensive period. The substantial investment required leads to many organizations being reluctant to embark on a long path of IT governance implementation. Despite the importance of IT governance frameworks, little empirical research has been carried out on developing ways in which to effectively implement, maintain, and evaluate IT governance programs (Bermejo, Tonelli, Zambalde, Santos, & Zuppo, 2014).

Significant focus has been placed on the development of IT governance standards and models. This suggests that the current challenges of IT governance are not the absence of standards or models, but rather the absence of an effective and practical strategy for successfully assessing IT governance. In particular, there is little research in the literature that analyzes COBIT or uses COBIT as a tool for implementing research programs. To facilitate effective IT governance implementation, the maturity of organizations should be measured by using IT governance evaluation methods (De Haes & Van Grembergen, 2005). These evaluation methods are often based on a more or less comprehensive set of criteria and provide a way of scoring the capability of IT governance processes (Cadete & da Silva, 2017). However, organizations generally adopt ad hoc methods instead of standard methods to assess IT governance. Therefore, IT governance assessment methodologies need to be adjusted according to their applicability in a specific area and sector (Tonelli, de Souza Bermejo, Aparecida dos Santos, Zuppo, & Zambalde, 2017). Therefore, we argue that it is necessary to contextualize the use of COBIT before it can be properly applied to assess IT governance in any industry. This has the potential to reduce the time and cost of assessing IT governance and to provide more contextualized methods (Omari, Barnes, & Pitman, 2012).

The major challenges of IT governance are the lack of practical methods to contextualize or adapt evaluation frameworks, particularly in specific contexts, and the lack of understanding of the adoption of the framework, particularly the factors that influence its adoption. Therefore, the aim of this chapter is to determine the main areas of adoption of IT governance, based on the COBIT standard in order to provide a practical and efficient framework to evaluate IT governance in medium and large organizations.

The remaining sections of this chapter present the background and the literature review in the next Section. Section 2 describes the theoretical framework. An overview of the research methodology will be presented in

section 3 and the contribution of the chapter in Section 4. The proposed case study will be described in section 5. Section 6 provides the chapter conclusion.

BACKGROUND AND LITERATURE REVIEW

IT governance is considered a complex system as it includes several critical aspects, namely, leadership, organization and decision rights, scalable processes and enabling technologies (Selig, 2008). Early conceptualisations of IT governance, often considered as a subset of corporate governance (De Haes, Van Grembergen, & Debreceny, 2013; Posthumus, Von Solms, & King, 2010), recognised the role of IT governance in ensuring a valuable contribution from the organisation's IT to its overall business strategy. More specifically, the role of IT governance is to "ensure that the organization's IT sustains and extends the organization's strategies and objectives" (ITGI, 2003).

A number of highly respected organizations and authors have attempted to define IT governance (Simonsson & Johnson, 2006), but as at the date of this chapter, there is not a commonly accepted universal definition of IT governance. IT governance can be defined as the process of controlling an organization's IT resources (Hunton, Bryant & Bagranoff, 2004). The International Standard for ICT Corporate Governance extends this definition to indicate that IT governance is the system by which the current and future use of ICT is directed and controlled. This involves assessing and guiding ICT use plans to support the organization and monitoring ICT use to achieve the plans. It includes the strategy and policies for using ICT within an organization (ISO, 2008).

As a result, IT governance has become a common component of most organizations' governance, oversight, and control landscapes (Schubert, 2004). As with most social phenomenon, the increasing importance of IT governance has given rise to several industry frameworks, tools, best practices, and maturity models, each offering a prescriptive and deterministic approach to establishing effective IT governance. Nonetheless, the significant role of frameworks has been established as an effective approach to IT governance (Guldentops, 2002; Webb, Pollard, & Ridley, 2006) by way of providing guidance to organisations and offering an advantage as compliance with these standards allows the enterprise to demonstrate they are following best practices and complying with regulatory rules (Brown, Grant, & Sprott, 2005a). For example, prominent meta-frameworks such as ISO 38500 and ITIL provide a comprehensive suite of best practices for standardizing, monitoring, and

controlling IT activities (Wallhoff, 2004). However, guidance on IT governance can perhaps be better found through the Information Systems Audit and Control Association (ISACA) and its related professional organization, the IT Governance Institute (ITGI) (Moeller, 2011).

COBIT is a set of best practices developed by ITGI and is widely accepted as the main IT governance framework for establishing control over the IT environment, facilitating performance measurement of IT processes and allowing executives to bridge the gap between control requirements, technical issues, and business risks (Aebi, Sabato, & Schmid, 2012; Kaen, 2005).

Given the varied and significant organisational pressures to ensure proper oversight and control of IT, it is interesting to note that, despite the considerable academic and practitioner focus on COBIT as a de facto framework for IT governance over the last two decades (Brown, Grant, & Spratt, 2005b; De Haes et al., 2013; Guldentops, 2002; Webb et al., 2006). Many organizations continue to struggle with fundamental governance practices, such as appropriately selecting, implementing, managing, and evaluating IT governance processes (Heier, Borgman & Mervyn, 2007; McKay, Marshall, & Smith, 2003).

From an anecdotal perspective, COBIT's size, and multifaceted and complex structure make implementing a framework of this magnitude in its entirety too medium and large a task (Steven De Haes et al., 2013; Warland & Ridley, 2005). This is also echoed by statements that view the COBIT framework as being too extensive to be completely applied and proposed to move to a less complex approach to defining and establishing selective controls. Prominent researchers in the domain, (De Haes & Van Grembergen, 2005; Peterson, 2004; Webb et al., 2006; Weill & Ross, 2005) all put forth converging definitions of IT governance that recognizes the importance of all three structural, process, and relational mechanisms. Although the value of user involvement in various aspects of IT governance has long been recognised (Posthumus et al., 2010; Van Grembergen, 2004), human behaviour aspects of IT governance has received far less attention from academics (El-Mekawy, Rusu, & Perjons, 2015; Lengnick-Hall, Beck, & Lengnick-Hall, 2011).

The importance of IT governance and the relevance of frameworks provide the context for this study, which also focuses on the factors underlying the adoption of IT governance frameworks. In particular, the intentions and opinions of the adopters are explored to shed light on the factors influencing adoption intent.

Several studies have endeavored to tailor and adapt the COBIT framework for a specific organizational context. For example, a study by Nugroho (2014) examined COBIT 5 as an IT governance tool in higher education institutions

in Indonesia. The author concluded that each organization must take into account its specific situation to define its own set of governance processes as it sees fit, as long as all necessary governance and management objectives are covered. Similarly, Hiererra (2012) conducted a focused evaluation using eight high-level control objectives from COBIT to determine the IT governance maturity of the information systems (IS) department within a single university in Indonesia. Along the same line, a study by Wood (2010) adopted a case study design based on nine of the COBIT high-level control objectives as a modified framework to evaluate the IT governance maturity of the city of San Marcos in the United States. Similarly, the implementation of COBIT as an IT governance framework was examined in an educational institution in Portugal by Gomes and (Ribeiro & Gomes, 2009) and also in two Australian institutions of higher education by Bhattacharjya and Chang (2010).

In a similar effort to derive an abbreviated list of IT processes for creating an integrated IT governance framework in the Malaysian Ministry of Education, (Azizi Ismail, 2008) noted that the focus on IT governance domains differ between different parts of the organization. For example, the Plan and Organize domain was the main focus at the ministerial level, whereas the Monitor and Evaluate domain was given the highest emphasis at the schools level. Their study concluded with determining 20 high-level control objectives that were considered to be most important in one organization. Similarly, Braga (2015) recommended adopting COBIT for private sector organizations in Argentina. The author utilized the framework's goals cascade mechanism to pick a specific set of primary and secondary processes that relate to two IT-related goals: compliance with external regulations and laws; and security of information, processing infrastructure, and applications.

In the same vein, Al-Khazrajy (2011) indicated that COBIT helps in conducting IT governance evaluations at low cost with better value, as it can be tailored to fit certain organizational needs. However, none of these studies provided empirical evidence of the validity of their selection or practical methods for utilizing COBIT by auditors. As a result, it is proposed that tailoring the COBIT framework to conduct IT governance evaluation that is relevant to a specific organizational context is possible.

Afterward, Warland & Ridley (2005) conducted a study to establish a reference benchmark of maturity levels of control over IT processes in the Australian financial sector by adopting a self-assessment tool based on the study's selection of 15 controls from COBIT by Guldentops (2002) to elicit the level of control over IT processes. The authors then compared the Australian benchmark with the international benchmark established by Guldentops, (2002)

and concluded that the Australian financial sector had a better performance for IT control over the 15 most important IT processes. Subsequently, a study by Nfuka and Rusu (2010) also used the previously selected 15 processes from the COBIT framework to evaluate IT governance maturity in five Tanzanian public organizations and compared the results with those of previous studies of Gulentops (2002) and Warland and Ridley (2005).

They concluded that when the maturity levels in the studied environment were compared with those in the public sector in Australia and internationally in a range of nations, the maturity pattern appeared to be relatively lower in Tanzania as a developing country. As observed in the previous studies, the authors agreed on three points. First of all, only a limited number of empirical research studies exist that focus on the evaluation of IT governance using COBIT in the public sector environments worldwide. Second, the authors noted the similarity between the rankings of the leading IT processes, which suggests that the priority placed on these specific IT processes is medium and largely consistent.

This also indicates a consistency in the nature of the IT governance practices and maturity within the public sector worldwide. Third, none of the studies provided a justification or a mechanism for the selection of the leading (or most important) 15 IT processes from the COBIT framework. Another project was undertaken by the IT working group at the European Organization of Supreme Audit Institutions (EUROSAI) to design a self-assessment tool for evaluating IT governance based on the COBIT framework. Similar to the previous studies, a list of 16 key control objectives was identified as the most important to Supreme Audit Institutions (Huissoud, 2005). In the same way, a study was undertaken by Webb et al. (2006) in Australia to identify and assess a set of control objectives to be used as an IT evaluation instrument by the Tasmanian Audit Office within public organizations. The authors produced an abbreviated list of 17 high-level control objectives from the COBIT framework that were considered to be important to Tasmanian organizations.

THEORETICAL FRAMEWORK

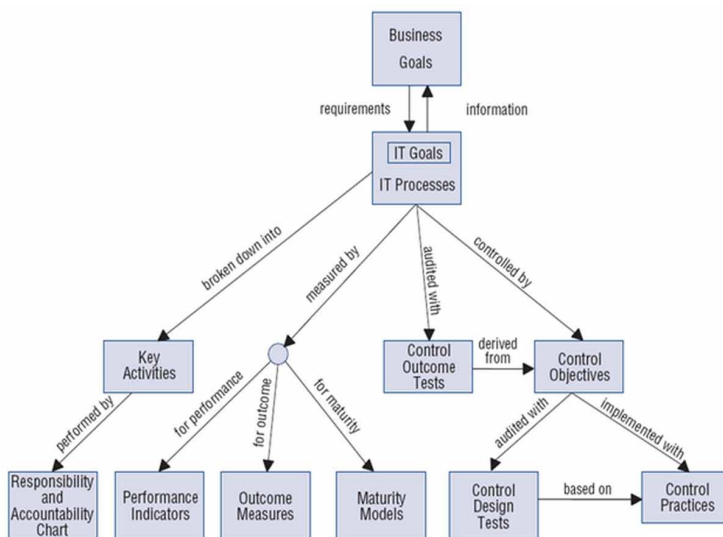
The COBIT framework recognizes the importance of effectively assessing IT governance to organizations by articulating that a basic need for every enterprise is to understand the status of its own IT systems and to decide what level of management and control the enterprise should provide (“Information Security Governance,” 2006). It also notes that the assessment of process

capability based on the COBIT maturity models is a key part of IT governance implementation as shown in Figure 1.

Although obtaining an objective view of an organization’s own IT performance level through maturity models has been described as a challenging undertaking, COBIT enables measurement of IT capability as a portfolio through assessing the maturity of individual IT processes (Chen, Sun, Helms, & (Kenny) Jih, 2008). Evaluating IT governance can be based on the Process Capability Model (PCM) or the generic maturity model (in previous versions of COBIT), with selected or all 37 IT processes (“Information Security Governance,” 2006). For example, De Haes et al. (2013) undertook a medium and large field study to evaluate the maturity of IT processes.

The authors used all 34 processes in COBIT 4 as a foundation to evaluate process capability by interacting with process owners at 52 organizations in several countries. The authors applied an extensive survey instrument, which found that the mean level of process maturity is rather low, with higher process maturity being observed in more operational processes. However, the authors concluded that exploiting the COBIT framework in its entirety was too generic and as a result may not have directly correlated to the capabilities of any particular organization. On the other hand, Weber (2014) developed an evaluation framework based on a selection of processes to be used in South African organizations. The author concluded that the use of

Figure 1. COBIT governance model



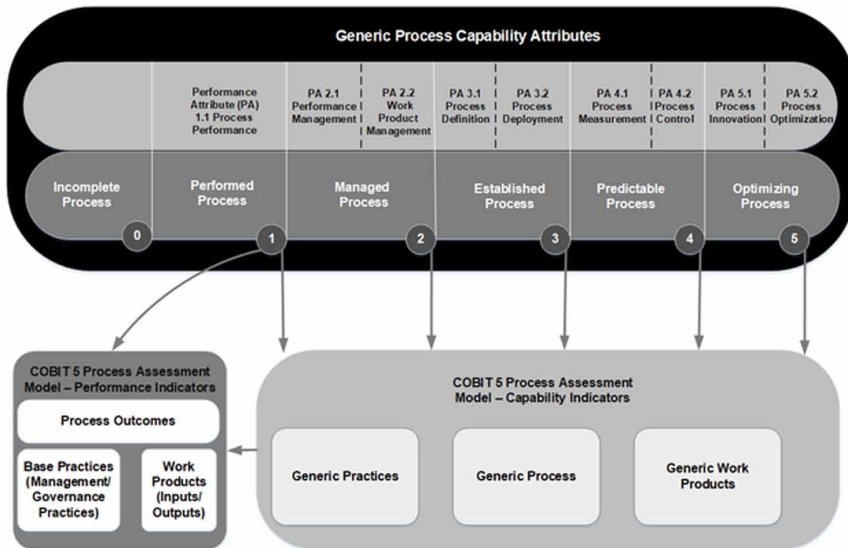
a selection of processes from COBIT 5 produced an acceptable and fit-for-purpose framework to use in evaluating ITG.

The process capability model PCM utilized in COBIT provides a structured approach for IT capability assessment through evaluating processes capability against a consistent and well-established scale (Oliver & Lainhart, 2012). The evaluation is performed through metrics that assess a unique set of key goal indicators (KGIs) and key performance indicators (KPIs) for each IT process. KGIs are lead indicators that aim to identify and measure the application of processes. On the other hand, KPIs are lag indicators that assess the achievement of process goals. KPIs and KGIs are often associated with Balanced Scorecards (BSC) and are important in measuring the relationship between IT processes and business goals which is critical to the success of ITG. For all 37 IT processes a set of IT-related goals (i.e., to define what IT objectives are achieved by the process), process goals (i.e., to define what IT must deliver to support objectives), and activities (i.e., to assess actual performance) is provided.

According to ISACA (2012), there are six levels of capability that a process can achieve in COBIT as shown in Figure 1:

- **Incomplete (Level 0):** The process is not implemented or fails to achieve its objective. This level has no process attributes.
- **Performed (Level 1):** The process is implemented and achieves its objective. This level has only one process attribute: process performance.
- **Managed (Level 2):** The previously described performed process is now implemented using a managed approach and its outcomes are appropriately established. This level has two process attributes: performance management and work product management.
- **Established (Level 3):** The previously described managed process is now implemented using a defined process that is capable of achieving its process outcomes. This level has two process attributes: process definition and process deployment.
- **Predictable (Level 4):** The previously described established process now operates within a defined boundary that allows the achievement of the processes outcomes. This level has two process attributes: process management and process control.
- **Optimizing (Level 5):** The process is continuously improved in a way that enables it to achieve relevant, current, and projected goals.

Figure 2. Summary of the COBIT 5 process capability model (ISACA, 2012)



This level has two process attributes: process innovation and process optimization.

Furthermore, each capability level can be achieved only when the level below has been fully achieved as shown in Table 1. For example, a process capability level 4 (predictable) requires the process management and process control attributes to be medium and largely achieved, on top of full achievement of the attributes for a process capability level 3 (established).

The COBIT framework was selected for use in this research as it was derived specifically to guide the practice of IT governance and is used extensively throughout the public and private sectors for this purpose. It is important to note that in many previous studies the decision to utilize all or a collection of IT processes from COBIT was based on the opinion of the researchers. As a result, no consistency for the selection of specific IT processes was provided for a given context, which also makes it difficult to compare results. Consequently, the next section explores previous studies that have attempted to adapt the COBIT framework for conducting an evaluation of IT governance.

Table 1. COBIT 5 process capability levels (ISACA, 2013)

		Processes exists?	Process Attribute								
			PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Process Capability Level	Level 5 (Optimized)	Yes	L or F	L or F	L or F	L or F	L or F	L or F	L or F	L or F	L or F
	Level 4 (Predictable)	Yes	L or F	L or F	L or F	L or F	L or F	L or F	L or F		
	Level 3 (Established)	Yes	L or F	L or F	L or F	L or F	L or F				
	Level 2 (Managed)	Yes	L or F	L or F	L or F						
	Level 1 (Performed)	Yes	L or F								
	Level 0 (Incomplete)	NO									
Rating scale:	N: Note achieved (0-15%)										

RESEARCH METHODOLOGY

Despite its prevalence in practice, little academic literature has been published on adapting and adopting best practice frameworks and models for assessing IT governance. It is necessary to understand whether theoretical constructions of information systems (IS) can be useful in understanding the adoption of the IT governance framework and how these factors can guide developers and proponents of contextualized frameworks. More formally, the overarching research question for this research is: How can best practice frameworks be adapted and adopted to assess IT governance in medium and large organizations across all sectors? The secondary research questions are as follows: Question1. Which are the pertinent process that can be adapted to conduct IT governance assessments in medium and large organizations? Question2. How can medium and large organizations assess IT governance using appropriate best practice frameworks?

A mixed-approach was adopted because this conception is clearly linked to the research paradigm of “realism” chosen for this research. As critical realism, research methods were chosen based on the nature of the research problem (McEvoy & Richards, 2006). Therefore, a mixed approach, which

combines quantitative and qualitative methods, is considered the most effective strategy for this research (Perry, Alizadeh & Riege, 1997). By applying both approaches at different stages of the research program, the researcher was able to collect data on the same questions from different sources, which could be triangulated together. This approach also reduces the weaknesses associated with using a single method (Charles & Tashakkori, 2009). In addition, a mixed approach is considered most appropriate for exploring the research question “How to adapt and adopt best practice frameworks to assess IT governance in medium and large organizations”, as the implementation of multiple methods across a number of steps or research activities helps answer this type of general question (Morse & Niehaus, 2009). From a theoretical perspective, a mixed approach gave this research the best chance to discover the theoretical mechanisms underlying the contextualization and adoption of IT governance frameworks (Charles & Tashakkori, 2009). A combination of quantitative and qualitative methods has been designed to lead to a thicker and deeper understanding of the research question (Creswell & Creswell, 2017). As the research progressed, the design of mixed methods developed so that the results of the first phase, including three research activities or studies, contributed to the development of a more in-depth study of the drivers of innovation adoption and IT governance frameworks in the second phase (Charles & Tashakkori, 2009). In addition, the mixed approach allowed this research to develop from the literature on IT governance and innovation adoption theories, and thus this research is considered from a unified position. Therefore, this research is able to combine the strengths of quantitative research with those of qualitative research to deepen understanding of a complex phenomenon.

A number of obvious gaps emerge from previous research with respect to exploring the challenges of assessing IT governance, particularly appropriate governance frameworks, or rather the lack of governance frameworks, in medium and large organizations. There is also a gap in the study of the methodological adaptation of the COBIT framework to the specific needs of individual organizations or sectors. Therefore, this research seeks to address the gaps identified in the area of IT governance by answering the primary research question: “How can best practice frameworks be adapted and adopted to assess IT governance in financial sector organizations?”

The primary research questions are as follow:

- **Research Activity 1:** Which are the best process that can be adapted to conduct IT governance assessments in medium and large organizations? This question aims to address one of the key IT governance assessment

challenges identified. While there may be several ways to do this, as an intervention in this research, IT governance frameworks, particularly COBIT, have been taken into account because of the need highlighted in the literature to focus on contextualization (or adaptation) as an important research area. In order to make optimal use of scarce medium and large organizations resources in an effective and efficient manner.

- **Research Activity 2:** How can medium and large organizations evaluate IT governance using adapted best-practice frameworks? A method with guidelines in the form of an evaluation framework for IT governance was tested. The research activity evaluated IT governance in a medium and large organization in terms of the capability levels of their IT processes.

Embarking on a research project requires the investigator to have a clear picture of the research process and associated activities. The research methodology and approach must be carefully planned and formulated to provide the information required to successfully answer the research questions and solve the research problem. To explore whether the COBIT framework can be adapted and adopted to conduct an evaluation of IT governance in the Middle East and North Africa MENA Port organizations from different sectors, the researchers employed a two-stage mixed-methods approach that evolved over time.

Generally, two research approaches are often employed by social science research studies including information systems (IS), namely, quantitative and qualitative. Typically, researchers choose one or both of these two approaches (also known as mixed methods) depending on the problem definition (Punch, 2013). Although research studies can be generally classified as having a more qualitative or quantitative focus in nature, the distinction between the two methods has become less clear and can usually be more accurately described as representing different ends on a continuum (Creswell & Creswell, 2017). This study adopted a mixed-methods approach because it is a suitable fit within the realism paradigm and provides the depth dictated by the nature of the research problem. This approach assisted in attaining a better understanding of the research problem and leverage the most appropriate tools for the research questions. In addition, using a mixed-methods approach provided an opportunity to minimize flaws associated with using qualitative methods (e.g., lack of generalisability) and quantitative methods (e.g., lack of context understanding) individually, as embracing a blend of qualitative and quantitative approaches will draw from the strengths and mitigate the

weaknesses of both. Similarly, Charles and Tashakkori (2009) suggest that linkages between qualitative and quantitative methods will reduce bias in the results and mutually strengthen the findings from both approaches. The mixed-methods approach was essential in understanding the evaluation of IT governance processes, customized IT governance frameworks, and the factors impacting the adoption of information systems related innovation in the financial sector environment. Published mixed-methods studies (De Haes & Van Grembergen, 2006; Hiererra, 2012; McEvoy & Richards, 2006; McGuire, 2016) suggest that social researchers use mixed methods approaches for one or more of the following purposes: providing a more complete picture; improving accuracy; compensating for strengths and weaknesses; and, more importantly, developing robust analysis (Denscombe, 2014).

In the first research activity, we utilized a quantitative survey that aimed at developing an evaluation framework for IT governance in medium and large organizations. An online questionnaire was developed to gather respondents' perceptions of the importance of each of the 37 high-level IT processes from the COBIT framework. Given the findings from the previous research activities, the second research activity was designed to evaluate IT governance processes using the adapted framework by applying a case study research in a medium and large organization in Morocco. The case study was selected for a number of reasons. (i) According to Hancock and Algozzine (2016), case study research emphasizes studies in natural settings and allows for greater understanding of the context in which a phenomenon exists through the collection of rich data from which to draw conclusions. IT governance is a phenomenon that occurs within the context of the organization and is the unit of analysis. (ii) Case studies not only allow the exploration of the individual participant's viewpoint but also various groupings of participants (Cronin, 2014). The use of multiple sources of data from the perspective of various stakeholders was required to ensure an accurate evaluation of IT governance processes. (iii) Case study research is suitable for dynamic organizations investigating emergent and rapidly evolving phenomenon. The examined company is considered a dynamic organization, with IT governance being an emergent and rapidly evolving phenomenon. (iv) Case studies can investigate and describe the processes and underlying meaning of current events through collecting and integrating quantitative survey data, which facilitates reaching a holistic understanding of the phenomenon being studied (Lewis, 2015). Based on applied research methods, this research could have utilized a number of data collection techniques, including interviews, survey questionnaires, and documents review (Hyett, Kenny, & Dickson-Swift, 2014). Although the

choice of using one or a combination of these techniques depends on the goal of the research activity, initial discussions with potential participants from the MENA Port organizations revealed that they opposed participating in interviews and would prefer to respond to anonymous questionnaires instead. As a result, the two research activities utilized questionnaires as a main data collection technique. In this research, it was applied to research activities 1 and 2 to analyze data that were obtained from the questionnaires. This mainly involved measures related to relative location, such as rankings, and those related to the center, such as means. Structural equation modeling is better known as a data analysis tool for testing and estimating causal relationships in quantitative research studies.

EXPLORING IT GOVERNANCE IN MENA MEDIUM AND LARGE ORGANIZATIONS

We have carefully identified 20 medium and large Port organizations in the MENA region (Morocco, Algeria, Tunisia, UAE, Saudi Arabia and Kuwait) that are either fully or partially implemented COBIT. Since this research is exploratory in nature, we have used a qualitative research method using the 10 organizations as case studies to identify the best practices for implementing COBIT. The above approach enabled us to inquire and ask questions with the aim to capture the contributor's rich knowledge, experience and views.

We have conducted case semi-structured interviews with the organization's IT service managers. Due to the business sensitivity of the information and comments, the real business names of the organizations can't be revealed. The 10 organizations are referred to throughout the research discussion as cases A-E. Table 1 presents each organization in terms of nature, size, COBIT version, knowledge and experience of COBIT within the staff, the phase of COBIT implementation and the motivation of COBIT implementation. COBIT professionals in these organizations were interviewed and questioned. The interview questionnaire comprises two main parts: part 1 contains questions about the organization demographics (i.e. nature, size, number of IT employees, etc.). Part 2 covers questions about the best practice in implementing each process of the COBIT. Although questions of part b are used as a guide throughout the interviews we did not totally depend on these questions, other developed inquiries and thoughts during the interviews were also discussed.

Subsequently, an online questionnaire was developed consisting of asking participants to rate the 37 high-level IT processes and 210 practices from the COBIT 5 framework according to their importance to the MENA Port organizations on a five-point Likert-type scale.

Data Collection

The targeted population included participants at different levels (c-suite, managers and senior IT, audit and business officers) who have knowledge of IT governance within the MENA Port organizations. Support was gained from the aforementioned groups to email a personal invitation to potential participants containing a link to the online questionnaire and an information research sheet (for the right of usage ISACA, we don't include the questionnaire).

The selected organizations invited to participate were advised that the origin and details of individual respondents would not be directly identified in any publication or other material arising from the research. This was considered an important factor in the success of the research, as obtaining the CIOs' permission conveyed top management support for the study. Participating organization returned this information and the persons nominated by the organization was emailed a personal invitation outlining the research study, its motivation, and information about the interview process. Data collection processes were designed to evaluate the levels of IT governance processes in MENA Port organizations using COBIT 5. Initially, a semi-structured, open-ended data collection instrument and interview protocol were developed for this research activity. However, on contacting nominated respondents to arrange a suitable time and place for the interview, every one of them indicated that they were, although keen to assist, uncomfortable with participating in a face-to-face interview and would prefer to respond to an anonymous questionnaire instead. As a result, the researcher decided to utilize an online questionnaire as a data collection instrument. A questionnaire was considered an appropriate method to collect perceptions of capability levels from respondents within the organizations. A principal advantage of this technique was the ability to cost-effectively collect data in a timely fashion from a significant number of organizations. Where the data was collected from more than one person for a given process, the between-person variation was typically within one level of maturity. Data are, of course, self-reported and subject to bias.

The data were collected from the employees of 10 different companies who had established proper information governance through COBIT in MENA Ports

from the beginning of June 2017 to the end of November 2017 and a total of 400 emails were distributed. Follow-up emails were sent to encourage non-respondents to participate and a total number of 160 responses were received. However, only 122 complete surveys were included as only completed surveys were considered in the final analysis. The response rate at 80 valid responses was 66%, which is considered above average for academic research and thus representative of the whole population (Baruch & Holtom, 2008). The release of COBIT 5 in April 2012, shortly before starting data collection, might explain the good response rate for this research, suggesting it was recognized as both credible and relevant to the public sector. The demographic data derived from the first section of the questionnaire comprised an organizational type, respondent’s position level, familiarity with IT processes, and familiarity with the business goals of the organization. This provides a context for the data obtained from the second section of the questionnaire, the rating of the high-level COBIT IT processes. Table 2 shows the summary of key attributes of medium and large organizations cases.

Data Analysis

This research aims to present a conceptual framework that shows how information governance through COBIT 5 arises in organizations. The data were collected by means of a Likert scale and questionnaires. The items for each construct are adopted from previous studies and each question relates to an item (Bergner, Witherspoon, Cockrell, & Stone, 2013; Pat & Piattini,

Table 2. Summary of key attributes of MENA port organizations cases

Organizations	A	B	C	D	E	F	G	H	I	G
No of employees	1125	3500	2400	7000	12000	8920	5245	2400	1700	22500
No of IT employees	80	280	190	220	420	240	115	44	35	360
Government (Gov.)/ Multinational (multi.)	Gov.	Multi.	Gov.	Gov.	Gov.	Multi.	Multi.	Gov.	Gov.	Multi.
COBIT Version	V4	V5	V4	V4	v V5	V5	V5	V5	V4	V5
Knowledge of COBIT with IT staff/Familiarity	30%	70%	45%	25%	60%	50%	60%	70%	34%	65%
Certified COBIT staff	5%	15%	5%	0%	10%	15%	20%	5%	0%	10%
Stage of COBIT Implementation	P	L	F	P	L	L	F	P	P	L
(Fully (F), largely (L), Partially (P))										

2011). To estimate the extent of non-respondent bias, it was not possible to compare respondents with non-respondents' answers. This is because the survey was anonymous and we had access only to names and e-mail addresses of participants, unlinked to their responses, and not those who chose not to participate. As a result, a non-response bias test was undertaken by comparing early respondents with late respondents instead (Lewis-Beck, Bryman & Liao, 2003).

Overall, in view of the preliminary nature of this study, the non-response bias test and response rates reported in information systems (IS) research, the 80 responses can be considered as a reasonable sample.

Table 3. Rating for COBIT 5 high-level IT processes as perceived by MENA port organizations

Domain	Process ID	Process	Mean	T stat	P
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	4.86	1.05	0.23
Evaluate, Direct and Monitor	EDM02	Ensure Benefits Delivery	5.13	1.76	0.09
Evaluate, Direct and Monitor	EDM03	Ensure Risk Optimisation	5.21	0.85	0.19
Evaluate, Direct and Monitor	EDM04	Ensure Resource Optimisation	4.91	0.52	0.37
Evaluate, Direct and Monitor	EDM05	Ensure Stakeholder Transparency	4.39	0.61	0.37
Align, Plan and Organise	APO01	Manage the IT Management Framework	4.61	2.21	0.09
Align, Plan and Organise	APO02	Manage Strategy	4.96	0.87	0.22
Align, Plan and Organise	APO03	Manage Enterprise Architecture	4.40	0.39	0.29
Align, Plan and Organise	APO04	Manage Innovation	3.89	1.92	0.02
Align, Plan and Organise	APO05	Manage Portfolio	4.13	1.35	0.08
Align, Plan and Organise	APO06	Manage Budget and Costs	4.84	1.35	0.09
Align, Plan and Organise	APO07	Manage Human Resources	4.17	2.07	0.08
Align, Plan and Organise	APO08	Manage Relationships	3.78	0.65	0.41
Align, Plan and Organise	APO09	Manage Service Agreements	3.84	0.24	0.47
Align, Plan and Organise	APO10	Manage Suppliers	3.92	1.54	0.06
Align, Plan and Organise	APO11	Manage Quality	4.54	0.96	0.21
Align, Plan and Organise	APO12	Manage Risk	5.02	1.86	0.05

continued on following page

Evaluation of IT Governance in Middle East and North African Large Organizations

Table 3. Continued

Domain	Process ID	Process	Mean	T stat	P
Align, Plan and Organise	APO13	Manage Security	5.25	1.15	0.13
Build, Acquire and Implement	BAI01	Manage Programmes and Projects	4.34	0.85	0.37
Build, Acquire and Implement	BAI02	Manage Requirements Definition	3.91	1.03	0.15
Build, Acquire and Implement	BAI03	Manage Solutions Identification and Build	4.05	1.86	0.12
Build, Acquire and Implement	BAI04	Manage Availability and Capacity	4.51	1.13	0.05
Build, Acquire and Implement	BAI05	Manage Organisational Change Enablement	4.05	1.94	0.08
Build, Acquire and Implement	BAI06	Manage Changes	4.85	0.85	0.27
Build, Acquire and Implement	BAI07	Manage Change Acceptance and Transitioning	4.03	0.78	0.31
Build, Acquire and Implement	BAI08	Manage Knowledge	3.98	1.05	0.19
Build, Acquire and Implement	BAI09	Manage Assets	4.63	1.56	0.31
Build, Acquire and Implement	BAI10	Manage Configuration	4.05	0.87	0.19
Deliver, Service and Support	DSS01	Manage Operations	4.65	0.65	0.27
Deliver, Service and Support	DSS02	Manage Service Requests and Incidents	5.12	1.04	0.06
Deliver, Service and Support	DSS03	Manage Problems	4.86	1.12	0.09
Deliver, Service and Support	DSS04	Manage Continuity	5.12	1.31	0.08
Deliver, Service and Support	DSS05	Manage Security Services	5.26	0.76	0.06
Deliver, Service and Support	DSS06	Manage Business Process Controls	4.03	1.76	0.17
Monitor, Evaluate and Assess	MEA01	Monitor, Evaluate and Assess Performance and Conformance	4.65	0.47	0.37
Monitor, Evaluate and Assess	MEA02	Monitor, Evaluate and Assess the System of Internal Control	4.37	0.83	0.21
Monitor, Evaluate and Assess	MEA03	Monitor, Evaluate and Assess Compliance with External Requirements	4.56	0.56	0.37

Results

To produce a ranked list of high-level IT processes, ratings from the second section of the questionnaire were analyzed to provide a total score, average, and standard deviation for each of the 37 high-level IT processes. Data were sorted in descending order based on the mean values. In case of matching

means, IT processes were then sorted in descending order based on the total values. The ranked list is presented in Table 3.

As part of the statistical analysis employed by this research, the ratings were subjected to the paired sample student's t-test to identify significant differences between high-level IT processes. The test commenced from the top of the list, the highest ranked high-level IT processes at $p < 0.05$ and 56 degrees of freedom, and continued until a group, or tier, was identified through detecting a significant difference. The test then recommenced using the first high-level IT processes in the next grouping as the point of comparison until the list of 37 high-level IT processes were exhausted and five groupings, or tiers, were identified.

Five groups of high-level IT processes were identified through the statistical analysis of the perceived ratings, presenting several points at which an adapted ITG framework could be formed. Previous research by (Guldentops, 2002) identified a list of 15 important control objectives, while the study by (Huissoud, 2005) classified 16 as being most important. The Australian study by (Warland & Ridley, 2005) derived an abbreviated list of 17 important control objectives, as perceived by the Tasmanian public sector. Based on these sources, it was proposed that the initial ITG framework for the MENA port organizations would be created using the first two tiers to give a size of 16 high-level IT processes as displayed in Table 4.

The high-level IT processes identified as being most important were drawn from four of the five broad domains in the COBIT 5 framework, namely:

- Evaluate, Direct and Monitor (EDM);
- Align, Plan and Organize (APO);
- Build, Acquire and Implement (BAI);
- Deliver, Service and Support (DSS);
- Monitor, Evaluate and Assess (MEA).

With the Monitoring domain seen as irrelevant and more focus given to the APO and DSS domains. This indicates a focus on early-cycle activities of IT governance instead of those concentrating on monitoring and evaluating. The abbreviated list initially derived contained 15 high-level IT processes. The high-level IT process is seen to be most important, DSS05 Manage Security Services, was the same as that identified by prior national and international studies.

The high-level IT processes common to at least four of the previous studies investigated as being important in other contexts and the initial list derived from this study were:

- Manage Security Services
- Manage Service Requests and Incidents
- Manage Security
- Ensure Risk Optimisation
- Ensure Benefits Delivery
- Manage Continuity
- Manage Risk
- Manage Strategy
- Ensure Resource Optimisation
- Ensure Governance Framework Setting and Maintenance
- Manage Problems
- Manage Changes
- Manage Budget and Costs
- Manage Operations
- Monitor, Evaluate and Assess Performance and Conformance
- Manage Assets

Given the similarities found between this research results and previous studies, the consistencies between the results supported the suggestion that the importance of some high-level IT processes is independent of geographical context. In view of the difference in the organizational setting between previous studies examined, the results also demonstrated clear evidence that the importance of some high-level IT processes is also independent of organizational type. As a result, this chapter concludes that an adapted ITGEF within the Australian financial sector can be derived from the COBIT framework based on the ten high-level IT processes identified to be both enduring and relevant across geographical and organizational contexts as presented in Table 4.

CASE STUDY

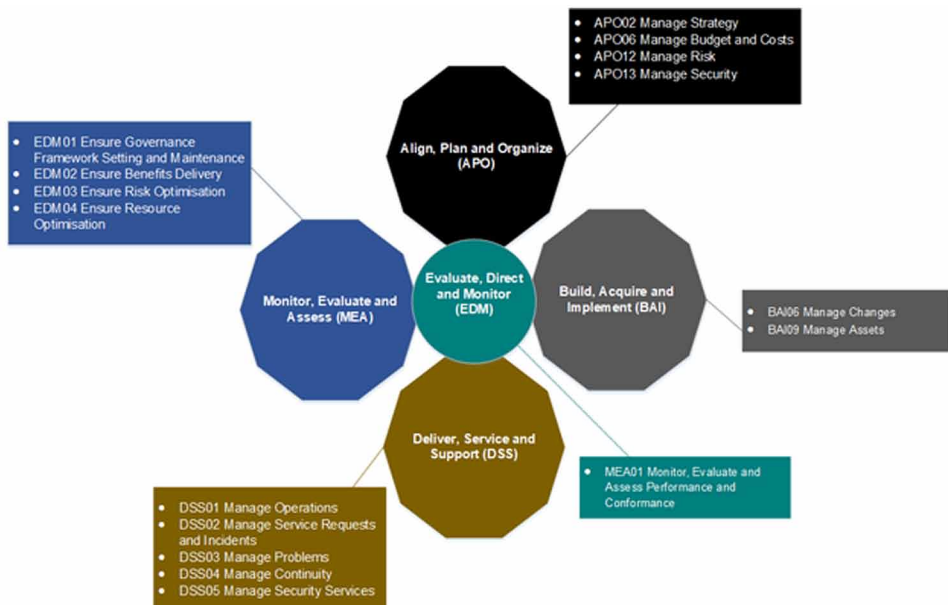
In order to gain a detailed understanding of the process for evaluating IT governance using the adapted IT Governance Framework based on the COBIT

Evaluation of IT Governance in Middle East and North African Large Organizations

Table 4. Top high-level IT processes for MENA port organizations

Domain	Process ID	Process
Deliver, Service and Support	DSS05	Manage Security Services
Deliver, Service and Support	DSS02	Manage Service Requests and Incidents
Align, Plan and Organise	APO13	Manage Security
Evaluate, Direct and Monitor	EDM03	Ensure Risk Optimisation
Evaluate, Direct and Monitor	EDM02	Ensure Benefits Delivery
Deliver, Service and Support	DSS04	Manage Continuity
Align, Plan and Organise	APO12	Manage Risk
Align, Plan and Organise	APO02	Manage Strategy
Evaluate, Direct and Monitor	EDM04	Ensure Resource Optimisation
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance
Deliver, Service and Support	DSS03	Manage Problems
Build, Acquire and Implement	BAI06	Manage Changes
Align, Plan and Organise	APO06	Manage Budget and Costs
Deliver, Service and Support	DSS01	Manage Operations
Monitor, Evaluate and Assess	MEA01	Monitor, Evaluate and Assess Performance and Conformance
Build, Acquire and Implement	BAI09	Manage Assets

Figure 3.



model, previously unexplored in the MENA port organizations, exploratory case study research was deemed appropriate.

Figure 3 shows the resultant conceptual framework for IT Governance.

Specifically, this research activity applied case study research considering that “where only limited theoretical knowledge exists on a particular phenomenon, an inductive research strategy can be a valuable starting point” (Siggelkow, 2007). An inductive, a case study strategy was adopted as it facilitates the identification of practical insights into IT governance evaluation frameworks. It also allows “replication logic”, whereby multiple cases are treated as a series of experiments, with each case serving to confirm, or not, the inferences drawn from previous cases (Yin, 2013). This approach also matches the research’s paradigm (i.e., realism) and adds credibility to the study (Tsang & Kwan, 1999). In addition, the use of case study research permits a flexible and thorough approach by employing a variety of data sources and

Table 5. Top high-level IT processes for MENA port organizations

Domain	Process ID	Process	Practice ID	Practice Name
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	EDM01.01	Evaluate the governance system.
			EDM01.02	Direct the governance system.
			EDM01.03	Monitor the governance system.
			DSS02.02	Record, classify and prioritise requests and incidents.
			DSS02.03	Verify, approve and fulfill service requests.
			DSS02.04	Investigate, diagnose and allocate incidents.
			DSS02.05	Resolve and recover from incidents.
Evaluate, Direct and Monitor	EDM02	Ensure Benefits Delivery	EDM02.01	Evaluate value optimisation.
			EDM02.02	Direct value optimization.
			EDM02.03	Monitor value optimization.
Evaluate, Direct and Monitor	EDM03	Ensure Risk Optimisation	EDM03.01	Evaluate risk management.
			EDM03.02	Direct risk management.
			EDM03.03	Monitor risk management.
Evaluate, Direct and Monitor	EDM04	Ensure Resource Optimisation	EDM04.01	Evaluate resource management.
			EDM04.02	Direct resource management.
			EDM04.03	Monitor resource management.

continued on following page

Evaluation of IT Governance in Middle East and North African Large Organizations

Table 5. Continued

Domain	Process ID	Process	Practice ID	Practice Name
Align, Plan and Organise	APO02	Manage Strategy	APO02.01	Understand enterprise direction.
			APO02.02	Assess the current environment, capabilities and performance.
			APO02.03	Define the target IT capabilities.
			APO02.04	Conduct a gap analysis.
			APO02.05	Define the strategic plan and roadmap.
			APO02.06	Communicate the IT strategy and direction.
			APO02.01	Understand enterprise direction.
			APO02.02	Assess the current environment, capabilities and performance.
			APO02.03	Define the target IT capabilities.
			APO02.04	Conduct a gap analysis.
			APO02.05	Define the strategic plan and roadmap.
			APO02.06	Communicate the IT strategy and direction.
Align, Plan and Organise	APO06	Manage Budget and Costs	APO06.01	Manage finance and accounting.
			APO06.02	Prioritise resource allocation.
			APO06.03	Create and maintain budgets.
			APO06.04	Model and allocate costs.
			APO06.05	Manage costs.
Align, Plan and Organise	APO12	Manage Risk	APO12.01	Collect data.
			APO12.02	Analyse risk.
			APO12.03	Maintain a risk profile.
			APO12.04	Articulate risk.
			APO12.05	Define a risk management action portfolio.
			APO12.06	Respond to risk.
Align, Plan and Organise	APO13	Manage Security	APO13.01	Establish and maintain an ISMS.
			APO13.02	Define and manage an information security risk treatment plan.
			APO13.03	Monitor and review the ISMS.
Build, Acquire and Implement	BAI06	Manage Changes	BAI06.01	Evaluate, prioritise and authorise change requests.
			BAI06.02	Manage emergency changes.
			BAI06.03	Track and report change status.
			BAI06.04	Close and document the changes.

continued on following page

Evaluation of IT Governance in Middle East and North African Large Organizations

Table 5. Continued

Domain	Process ID	Process	Practice ID	Practice Name
Build, Acquire and Implement	BAI09	Manage Assets	BAI09.01	Identify and record current assets.
			BAI09.02	Manage critical assets.
			BAI09.03	Manage the asset lifecycle.
			BAI09.04	Optimise asset costs.
			BAI09.05	Manage licenses.
Deliver, Service and Support	DSS01	Manage Operations	DSS01.01	Perform operational procedures.
			DSS01.02	Manage outsourced IT services.
			DSS01.03	Monitor IT infrastructure.
			DSS01.04	Manage the environment.
			DSS01.05	Manage facilities.
Deliver, Service and Support	DSS02	Manage Service Requests and Incidents	DSS02.01	Define incident and service request classification schemes.
				Define incident and service request classification schemes.
				Define incident and service request classification schemes.
				Define incident and service request classification schemes.
				Define incident and service request classification schemes.
				Define incident and service request classification schemes.
Deliver, Service and Support	DSS03	Manage Problems	DSS03.01	Identify and classify problems.
			DSS03.02	Investigate and diagnose problems.
			DSS03.03	Raise known errors.
			DSS03.04	Resolve and close problems.
			DSS03.05	Perform proactive problem management.
Deliver, Service and Support	DSS04	Manage Continuity	DSS04.01	Define the business continuity policy, objectives and scope.
			DSS04.02	Maintain a continuity strategy.
			DSS04.03	Develop and implement a business continuity response.
			DSS04.04	Exercise, test and review the BCP.
			DSS04.05	Review, maintain and improve the continuity plan.
			DSS04.06	Conduct continuity plan training.
			DSS04.07	Manage backup arrangements.
			DSS04.08	Conduct post-resumption review.

continued on following page

Table 5. Continued

Domain	Process ID	Process	Practice ID	Practice Name
Deliver, Service and Support	DSS05	Manage Security Services	DSS05.01	Protect against malware.
			DSS05.02	Manage network and connectivity security.
			DSS05.03	Manage endpoint security.
			DSS05.04	Manage user identity and logical access.
			DSS05.05	Manage physical access to IT assets.
			DSS05.06	Manage sensitive documents and output devices.
			DSS05.07	Monitor the infrastructure for security-related events.
Monitor, Evaluate and Assess	MEA01	Monitor, Evaluate and Assess Performance and Conformance	MEA01.01	Establish a monitoring approach.
			MEA01.02	Set performance and conformance targets.
			MEA01.03	Collect and process performance and conformance data.
			MEA01.04	Analyse and report performance.
			MEA01.05	Ensure the implementation of corrective actions.

research methods (Denscombe, 2014). Table 5 presented the selected Top high-level IT processes for MENA port organizations.

In the evaluation of IT governance using the COBIT framework, organizations make assertions about the way in which these IT governance processes are met. This is verified by internal or external auditors or by conducting self-assessments. The COBIT framework utilizes capability levels to assess IT processes on a scale from 0 (non-existent) to 5 (optimized).

Case selection involved three key decisions. First, a single sector was chosen to eliminate possible confounds that might arise from investigating multiple sectors. The research involved a large Port agency in Morocco, which were selected for a number of reasons:

The agency is highly dependent on IT to support their core functions. IT governance is likely to be a significant concern to these organizations and the study, therefore, more relevant. The agency is generally more supportive of research studies and consequently likely to assist in this study.

Data Collection

A case study was conducted as a pilot project to identify relevant ITG practices in the organization. The capability maturity framework is implemented at a leading port sector organization in Morocco. The organization manages more than 30 ports and sites with more than 12000 employees. The Information System department has 40 employees with different profiles. The purpose is to study IT governance practices. Figure 3 shows the ITG framework architecture proposed for an eventual implementation in the organization.

The respondents were asked to self-evaluate IT governance processes in their organizations based on the ITG framework, which contained sixteen high-level IT processes, as this approach was consistent with that of the original study (Gerke & Ridley, 2009). The guidelines provided through the “Process Assessment Model (PAM): Using COBIT 5” contained nine process capability levels to evaluate the IT governance processes of an organization as described. Taking one IT process at a time, the questionnaire introduces the process purpose and key practices from the PAM so that respondents could simply choose the process capability level for each of the nine attributes for that process.

However, face-to-face interviews have been scheduled with IT staff to assess the state of IT governance within the organization. For each organization, a maximum of 100 data points was collected, which represents achievement levels for ten attributes (nine process attributes + level zero criteria question), for the sixteen processes. When calculating the overall capability level for one process, the highest full or medium and large achievement level of the nine attributes associated with that process was taken. Similarly, a simple average of responses was calculated when more than one score was given. The capability levels for the sixteen most important IT processes reported a mean for each process.

This research activity also prepared and analyzed a list of possible process work products (WP) according to the evaluated IT processes (ISACA, 2013). The WPs included strategic and operational plans, structures, processes, policies, frameworks, service level agreements, performance reports, and so forth. The nominated WPs were included in the data collection instrument to elicit well-informed responses by respondents. For instance, in the process, APO02 Manage Strategy, respondents were instructed to consider the existence of a strategic IT plan as a work product of that process if it was the organization’s practice. In other words, this allowed the triangulation

of different data sources, thus adding to the credibility of the evaluated IT governance processes. The researcher was not able to validate independently the responses by inspection of each IT process WP listed or through other techniques. Therefore, based on the researcher's experience in the field, only two WPs were chosen and included in the questionnaire for each IT process as an indication of capability levels. The number of level 0 and level 1 responses received indicates the respondents seemed candid in the information they provided.

In the last section of the questionnaire, respondents were asked to rate the importance of 17 enterprise goals and 17 IT-related goals of IT governance of their respective organizations. This will assist in building a mapping between enterprise goals, IT-related goals, and IT governance processes similar to the goals cascade established by the COBIT 5 framework (ISACA, 2012b).

Before distributing the final version of the self-evaluation instrument, a web-based pilot was created. This pilot was posted online and two senior IT auditors were asked to complete it for a real-life situation. Based on their comments and suggestions, the instrument was made more user-friendly and accessible. Data collection for this research activity was performed in the period January–Mars 2018.

After data collection, a draft case report for each organization was sent back to respondents within that organization for review and confirmation.

The results for the position level of the respondents are presented in Table 6. From the 20 responses received, 15% (3 respondents) specified executive officer, 20% (4 respondents) specified officer, 30% (6 respondents) specified IT manager, 15% (3 respondents) specified Senior, and 20% (4 respondents) specified Auditor.

Table 6. Position level of respondents within the public sector

Executive Officer	3	15%
Officer	4	20%
IT Manager	6	30%
Senior Manager	3	15%
Auditor	4	20%

Table 7. Example of detailed IT governance process capability evaluation

Process name	Level 0		Level 1		Level 2		Level 3		Level 4		Level 5	
DSS05		Y/N	PA1.1	PA2.1	PA2.2	PA3.1	PA3.2	PA4.1	PA4.2	PA5.1	PA5.2	
Rating by criteria	Y		F	F	L	P	N					
Capability level achieved					2							
Rating scale:												
N: Not Achieved (0–15%)			P: Partially Achieved (15%–50%)			L: Medium and largely Achieved (50%–85%)				F: Fully Achieved (85%–100%)		

Data Analysis

The data collected from the questionnaire were analyzed using Microsoft Excel to establish the capability level of selected IT governance processes. MS Excel was selected as an exploratory data analysis tool because of the combination of its simplicity and its capability to calculate and present the results in tables and graphs. Specifically, respondents’ scores (from “not achieved” to “fully achieved”) for each attribute description of the evaluated IT process were incorporated into an Excel workbook (see Table 7 as an example). This was carried out for the key practices and statements of each capability level (from 0 to 5). Eventually, the capability level of each IT process was obtained. This was carried out for all ten IT processes in each studied organization.

All data collected analyzed in respect of each case study individually, across the case studies, and collectively for all case studies combined. The evaluation of the IT governance processes from this analysis is discussed further in the next section.

This study opted to distinguish between the utilization of maturity and capability levels as these terms were found to be used loosely in previous studies. Often considered as similar concepts, *organizational maturity* applies to an organization’s overall maturity and is concerned with evaluating a set of process areas across an organization, whereas *process capability* relates to evaluating a set of sub-processes and generic practices for a process area that can improve the organization’s processes associated with that area (Huang & Han, 2006). A maturity level results from aggregating the capability levels of all capability areas and demonstrates the extent to which an organization has developed its capabilities (Forstner, Kamprath, & Röglinger, 2014).

Evaluation of IT Governance in Middle East and North African Large Organizations

Table 8. Summary of capability levels for the ten most important IT processes (in order of priority) for Moroccan organization

Domain	Process ID	Process	Mean	Capability Maturity
Deliver, Service and Support	DSS05	Manage Security Services	2.2	2
Deliver, Service and Support	DSS02	Manage Service Requests and Incidents	3.8	4
Align, Plan and Organise	APO13	Manage Security	2.7	3
Evaluate, Direct and Monitor	EDM03	Ensure Risk Optimisation	1.7	2
Evaluate, Direct and Monitor	EDM02	Ensure Benefits Delivery	1.5	1
Deliver, Service and Support	DSS04	Manage Continuity	1.7	2
Align, Plan and Organise	APO12	Manage Risk	2.7	3
Align, Plan and Organise	APO02	Manage Strategy	1.5	1
Evaluate, Direct and Monitor	EDM04	Ensure Resource Optimisation	2.0	2
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	1.4	1
Deliver, Service and Support	DSS03	Manage Problems	2.3	2
Build, Acquire and Implement	BAI06	Manage Changes	2.0	2
Align, Plan and Organise	APO06	Manage Budget and Costs	2.0	2
Deliver, Service and Support	DSS01	Manage Operations	2.1	2
Monitor, Evaluate and Assess	MEA01	Monitor, Evaluate and Assess Performance and Conformance	1.8	2
Build, Acquire and Implement	BAI09	Manage Assets	2.6	3
Organisational maturity level			2.2	2

Assessing Capability Maturity

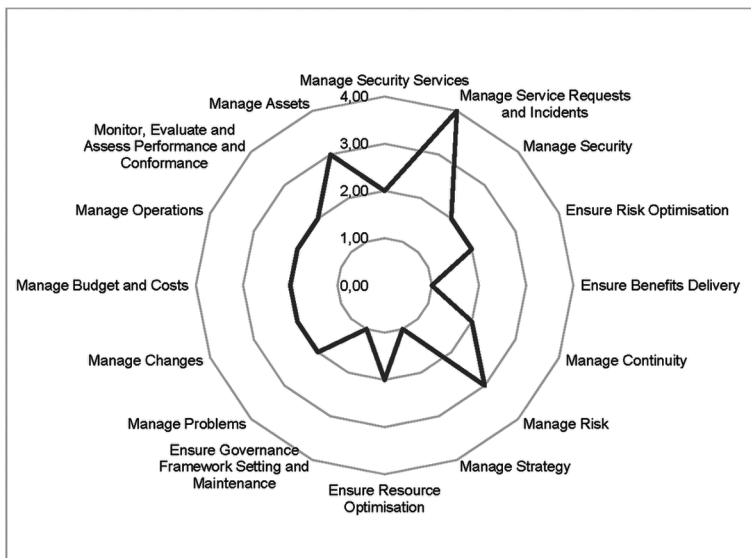
The analysis of the average maturity level across the studied organization involved calculating the average of each IT process capability level across these organizations. The averages provided the range within which the maturity levels of all assessed IT processes were calculated. The overall capability ratings of each IT process as evaluated by the respondents are presented in Table 8. The table also displays the means for the individual processes of each organization as well as the overall mean for each IT process.

The analysis of the organization maturity levels was carried out using the obtained capability level for each IT process from each organization’s point of view. Different from the previous one, the capability levels of IT processes were compared at the level of individual organizations. Such comparisons provided the relative evaluation of the processes in each organization and led to the individual organizations’ maturity levels for the adapted ITG framework based on the COBIT 5.

Capability Level Analysis

Figure 4 provides a box plot of the average capability level by the IT process. The mean capability level for all ten COBIT 5 processes is at level 2 (managed process) but with a significant variation (SD 0.89), which is strikingly clear from the whiskers in the box plots below. There are outliers at the lowest and highest levels of capability for each of these processes. As shown in Figure 4 there are clear differences between the sixteen most important processes. The average level of process capability scores is relatively low within the organization, with most processes having a mean capability level score between 1 (19%) and 2 (56%) on a scale from 0 to 5. Only 19% of the processes had a mean capability level of 3, while just 6% had a mean capability level of 4.

Figure 4. Range and distribution of capability level scores for the IT processes in the organization



Maturity Level Analysis

From a domain perspective, the Deliver, Service and Support (DSS) and Build, Align, Plan and Organise (APO) domains are perceived to have higher capability levels than the other three domains. Most of the processes in these domains are in the top quartile (DSS02 Manage Service Requests and Incidents), (APO13 Manage Security), (APO12 Manage risk), (BAI09 Manage Assets), (DSS03 Manage Problems), (DSS05 Manage Security services), (DSS01 Manage Operations), (APO06 Manage Budget and Costs), except (DSS04 Manage Continuity processes) and (APO02 Manage Strategy) from those two domains were in the lowest quartile of processes. An even more distinct result applies to the Evaluate, Direct, and Monitor (EDM) domain, with four process (EDM01 Ensure Governance Framework Setting and Maintenance (EDM02 Ensure Benefits Delivery), (EDM03 Ensure Risk Optimisation), and (EDM04 Ensure Resource Optimisation) being in the lowest quartile of capability. The more prosaic process has a relatively higher level of capability (EDM04 Ensure Resource Optimization). The Build, Acquire and Implement (BAI) domain was represented by two process (BAI06 Manage Change) and (BAI09 Manage Asset), which were in the lowest quartile of processes. The domain Monitor, Evaluate and Assess (MEA) was only represented by one process (MEA01 Monitor, Evaluate and Assess Performance and Conformance), which was in the top quartile of processes. considered of high importance by the organization.

Goals Cascade

The COBIT goals cascade mechanism that translates and links stakeholders' needs into specific enterprise goals, IT-related goals, and COBIT IT processes. The questionnaire asked respondents to rate the importance for each of the 17 enterprise goals and 17 IT-related goals from the COBIT 5 framework according to their importance to the organization a five-point Likert-type scale. The focus of this undertaking is not on enterprise goals or IT-related goals themselves, but rather to confirm, through the COBIT 5 goals cascade the importance of the adapted ITG framework for the MENA port organizations. The results were analyzed to produce a ranked list of enterprise goals and IT-related goals and to provide a total score and average for each of the enterprise goals and IT-related goals. The enterprise goals and IT-related goals ranked list is presented in Table 9 and Table 10 respectively.

Table 9. Rating for enterprise goals as perceived by the organization

Balanced Scorecard	Enterprise business Goal	Mean
Financial	1. Stakeholder value of business investments	4.48
	2. Portfolio of competitive products and services	3.96
	3. Managed business risk (safeguarding of assets)	4.40
	4. Compliance with external laws and regulations	4.32
	5. Financial transparency	4.16
Customer	6. Customer-oriented service culture	4.64
	7. Business service continuity and availability	4.32
	8. Agile responses to a changing business environment	4.28
	9. Information-based strategic decision making	4.16
	10. Optimisation of service delivery costs	4.40
Internal	11. Optimisation of business process functionality	4.28
	12. Optimisation of business process costs	4.36
	13. Managed business change programmes	3.96
	14. Operational and staff productivity	4.28
	15. Compliance with internal policies	4.20
Learning	16. Skilled and motivated people	4.40
	17. Product and business innovation culture	4.32

As part of the statistical analysis employed by this research activity, the ratings were subjected to the paired sample student’s t-test to identify significant differences between enterprise and IT-related goals. The test commenced from the top of the list, the highest ranked enterprise goal and the highest ranked IT-related goal both at $p < 0.05$ and 24 degrees of freedom and continued until a group, or tier, was identified through detecting a significant difference. The test then recommenced using the first goal in the next grouping as the point of comparison until the list of 17 business enterprises goals and 17 IT-related goals were exhausted and three groupings, or tiers, were identified for each category.

Three groups of enterprise and IT-related goals were identified through the statistical analysis of the perceived ratings, presenting several points at which a priority list for each category could be formed. However, as no previous research could be found in the literature to compare against and considering that the second tier in both lists contained at least 14 out of 17 goals, it was proposed that the perceived priority list of enterprise and IT-related goals for the MENA port organizations consist of those controls in the first tier

Evaluation of IT Governance in Middle East and North African Large Organizations

Table 10. Rating for IT-related goals as perceived by the organization

Process ID	IT-related goals	Mean
ITRG 01	Alignment of IT and business strategy	4.60
ITRG 02	IT compliance and support for business compliance with external laws and regulations	4.40
ITRG 03	Commitment of executive management for making IT-related decisions	4.68
ITRG 04	Managed IT-related business risk	4.52
ITRG 05	Realized benefits from IT-enabled investments and services portfolio	4.56
ITRG 06	Transparency of IT costs, benefits and risk	4.28
ITRG 07	Delivery of IT services in line with business requirements	4.44
ITRG 08	Adequate use of applications, information and technology solutions	4.16
ITRG 09	IT agility	4.32
ITRG 10	Security of information, processing infrastructure and applications	4.40
ITRG 11	Optimization of IT assets, resources and capabilities	4.36
ITRG 12	Enablement and support of business processes by integrating applications and technology into business processes	4.16
ITRG 13	Delivery of programs delivering benefits, on time, on budget, and meeting requirements and quality standards	4.44
ITRG 14	Availability of reliable and useful information for decision making	4.32
ITRG 15	IT compliance with internal policies	4.00
ITRG 16	Competent and motivated business and IT personnel	4.32
ITRG 17	Knowledge, expertise and initiatives for business innovation	4.36

only. That is, the priority list for the enterprise goals was made of six goals, whereas the same list for IT-related goals consisted of four.

The purpose of the mapping table in Table 10 is to demonstrate how enterprise goals are supported, or translate into, IT-related goals. Subsequently, Table 11 contains the mapping table between the IT-related goals and how these are supported by IT processes, as part of the goals cascade (ISACA, 2012). The results revealed that the required IT processes, a total of 28 IT processes, to support the perceived important IT-related goals for the MENA port organizations include the entire ITG framework total 16 IT processes, as perceived by the same sector. This validates the conceptual model for IT governance evaluation in organizations. This also allowed the triangulation of different data sources, thus adding to the credibility of the adapted ITG framework.

Evaluation of IT Governance in Middle East and North African Large Organizations

Table 11. Mapping enterprise goals to IT-related goals

IT goals	Business Goals	
Commitment of executive management for making IT-related decisions	<p>Most</p> <p>pertinent</p>	<p>Customer-oriented service culture</p> <p>Stakeholder value of business investments</p> <p>Managed business risk (safeguarding of assets)</p> <p>Optimisation of service delivery costs</p> <p>Skilled and motivated people</p> <p>Optimisation of business process costs</p> <p>Compliance with external laws and regulations</p> <p>Business service continuity and availability</p> <p>Product and business innovation culture</p> <p>Agile responses to a changing business</p> <p>Optimisation of business process functionality</p> <p>Operational and staff productivity</p> <p>Compliance with internal policies</p> <p>Financial transparency</p> <p>Information-based strategic decision making</p> <p>Portfolio of competitive products and services</p> <p>Managed business change programmes</p>
Alignment of IT and business strategy		
Realized benefits from IT-enabled investments and services portfolio		
Managed IT-related business risk		
Delivery of IT services in line with business requirements	<p>Pertinent</p>	
Delivery of programs delivering benefits, on time, on budget, and meeting requirements and quality standards		
IT compliance and support for business compliance with external laws and regulations		
Security of information, processing infrastructure and applications		
Optimization of IT assets, resources and capabilities		
Knowledge, expertise and initiatives for business innovation		
IT agility	<p>Least</p> <p>Pertinent</p>	
Availability of reliable and useful information for decision making		
Competent and motivated business and IT personnel		
Transparency of IT costs, benefits and risk		
Adequate use of applications, information and technology solutions		
Enablement and support of business processes by integrating applications and technology into business processes		
IT compliance with internal policies	<p>Least</p> <p>Pertinent</p>	

Discussion

The majority of recent IT governance research in the international scale has focused on accountability, decision-making requirements, structures and mechanisms, and factors reflecting localized contexts for adoption and implementation. However, a significant yet understudied aspect of IT governance is the capability of organizations to meet the ever-increasing resources and budget challenges by employing effective IT processes. Measuring IT process capability is considered important to ensure successful governance over IT. Nonetheless, very little empirical data on the level of process capabilities in the medium and large organizations context exist. In an effort to overcome this clear gap in the research literature, this research activity endeavored to seek support for and refinement of the ITG framework adapted from the COBIT model within selected state organizations and to compare the evaluation results with those obtained by other studies.

The adapted ITG framework contains six IT processes from COBIT that were also used by previous studies to conduct an evaluation of IT processes. These were:

- DSS05 Manage Security Services;
- APO13 Manage Security;
- EDM03 Ensure Risk Optimization;
- EDM02 Ensure Benefits Delivery
- DSS02 Manage Service Requests and Incidents;
- DSS04 Manage Continuity.

The remaining ten IT processes:

- DSS04 Manage Continuity;
- APO12 Manage Risk;
- APO02 Manage Strategy;
- EDM04 Ensure Resource Optimization;
- EDM01 Ensure Governance Framework Setting and Maintenance;
- DSS03 Manage Problems;
- BAI06 Manage Changes;
- APO06 Manage Budget and Costs;
- DSS01 Manage Operations;
- MEA01 Monitor, Evaluate and Assess Performance and Conformance;
- BAI09 Manage Assets.

We're not included in the previous studies, and so may reflect the particular needs of the MENA organizations that participated in this study.

The proposed framework was considered as appropriate by a number of methods, including triangulation and perceived relevance of the evaluation program. The trial of the ITG framework showed that it contained few evaluation measures that were not relevant to other jurisdictions in MENA or international organizations, which suggests that its development was appropriate. The results of this study show that

- The overall level of process capability in the MENA port organizations is relatively modest;
- Undertaking IT governance evaluation based on COBIT 5 is significantly more rigorous than earlier versions of the framework;
- There is considerable inter-process variability in capability levels as some processes that were expected to have a relatively high capability level were relatively underdeveloped;
- There is similar inter-organizational variation in process capability and maturity level within the MENA port organizations, which appears to be linked to the organizational size.

On that note, the results demonstrated that medium and larger organizations tend to have higher IT governance maturity than smaller organizations. Therefore, when studying organizations with approximately 10,000 employees, IT governance maturity levels of between 2.5 and 3 should be expected. Insufficient literature exists to determine whether that maturity level is sufficient or not.

In retrospect, it seems highly impractical for organizations to achieve capability level 5 in all process areas. So, what is the ideal capability level these organizations need to achieve for each process area? It appears that organizations can very well be successful with a capability level 2 or 3 for most process areas. Depending on business objectives or the type of services being offered, organizations can aim for specific process areas to be at a higher capability level. In other cases, there would be no incentive or a justified business case for trying to achieve a higher capability level for a given process area. The results suggest that the adapted version of the COBIT 5 model was fit for conducting an evaluation of IT governance and was contextualized to the needs of organizations. Accordingly, this study adds

credibility to the practitioner reports that it is possible to implement COBIT to produce an effective ITG framework that reflects the needs of individual organizations or sectors.

CONCLUSION

The primary objective of this research was to explore how best-practice frameworks, such as the COBIT model, can be adapted to conduct evaluations of IT governance within medium and large organizations and to further explore the factors that influence the acceptance and adoption of the adapted framework. Four sub-research questions were answered and a research model proposed and supported in order to address the primary objective of the research.

The research findings reinforce the important role of frameworks in IT governance evaluation. Employing an approach based on innovation adoption theory enables the understanding of the factors related to acceptance of IT governance frameworks, providing practitioners with additional knowledge and thus enabling a better understanding, and hence influencing, the adoption of IT governance frameworks.

In conclusion, taking into account the limitations identified, it is recommended that this research is extended to other organizations in both the private and public sectors. In addition, it is recommended that the research model is further developed to improve the quality of the findings and that more exploratory research is conducted on the relationship paths specified in the model.

In the next section, it propose 3 chapters to address the IT agility axis in large organizations. The first chapter of this section discusses the different models and frameworks of agility, the second focuses on IT service management agility through a case study, and the third chapter deals with the cloud-computing axis as a pillar of IT agility in organizations.

REFERENCES

Aebi, V., Sabato, G., & Schmid, M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance*, 36(12), 3213–3226. doi:10.1016/j.jbankfin.2011.10.020

- Al-Khazrajy, M. (2011). *Risk based assessment of IT Control Frameworks: a case study* (Master Thesis). Auckland University of Technology, Auckland, NZ.
- Al Omari, L., Barnes, P. H., & Pitman, G. (2012). An exploratory study into audit challenges in IT governance : a Delphi approach. In *Symposium on IT Governance, Management and Audit*. University of Tenaga Nasional.
- Azizi Ismail, N. (2008). Information technology governance, funding and structure: A case analysis of a public university in Malaysia. *Campus-Wide Information Systems*, 25(3), 145–160. doi:10.1108/10650740810886321
- Baruch, Y., & Holtom, B. C. (2008). Survey response rate levels and trends in organizational research. *Human Relations*, 61(8), 1139–1160. doi:10.1177/0018726708094863
- Beloglazov, A., Banerjee, D., Hartman, A., & Buyya, R. (2014). Improving Productivity in Design and Development of Information Technology (IT) Service Delivery Simulation Models. *Journal of Service Research*, 18(1), 75–89. doi:10.1177/1094670514541002
- Bergner, J., Witherspoon, C. L., Cockrell, C., & Stone, D. N. (2013). Antecedents of organizational knowledge sharing: A meta-analysis and critique. *Journal of Knowledge Management*, 17(2), 250–277. doi:10.1108/13673271311315204
- Bermejo, P. H. de S., Tonelli, A. O., Zambalde, A. L., dos Santos, P. A., & Zuppo, L. (2014). Evaluating IT Governance Practices and Business and IT Outcomes: A quantitative Exploratory Study in Brazilian Companies. *Procedia Technology*, 16, 849–857. doi:10.1016/j.protcy.2014.10.035
- Bhattacharjya, J., & Chang, V. (2010). Adoption and implementation of IT governance: cases from Australian Higher Education. In *Strategic Information Systems: Concepts, Methodologies, Tools, and Applications*. IGI Global.
- Braga, G. (2015). COBIT 5 Applied to the Argentine Digital Accounting System. *COBIT Focus*, 1–4.
- Brown, A. E., Grant, G. G., & Sprott, E. (2005). Framing the Frameworks: A Review of It Governance Research. *Communications of the Association for Information Systems*, 15, 696–712.
- Cadete, G. R., & da Silva, M. M. (2017). Assessing IT Governance Processes Using a COBIT5 Model BT - Information Systems. In M. Themistocleous & V. Morabito (Eds.), (pp. 447–460). Cham: Springer International Publishing.

Charles, T., & Tashakkori, A. (2009). *Foundations of mixed methods research: integrating quantitative and qualitative approaches in the social and behavioral sciences*. Academic Press.

Chen, R.-S., Sun, C.-M., Helms, M. M., & Jih, W.-J. (2008). Aligning information technology and business strategy with a dynamic capabilities perspective: A longitudinal study of a Taiwanese Semiconductor Company. *International Journal of Information Management*, 28(5), 366–378.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher*, 21(5), 19–27. doi:10.7748/nr.21.5.19.e1240 PMID:24877907

De Haes, S., & Van Grembergen, W. (2005). IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 237b–237b. 10.1109/HICSS.2005.362

De Haes, S., & Van Grembergen, W. (2006). Information technology governance best practices in Belgian organisations. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 8. 10.1109/HICSS.2006.222

De Haes, S., Van Grembergen, W., & Debreceeny, R. S. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems*, 27(1), 307–324. doi:10.2308/isys-50422

Denscombe, M. (2014). *The Good Research Guide: For Small-scale Social Research Projects* (5th ed.). Berkshire, UK: McGraw-Hill Education (UK).

El-Mekawy, M., Rusu, L., & Perjons, E. (2015). An evaluation framework for comparing business-IT alignment models: A tool for supporting collaborative learning in organizations. *Computers in Human Behavior*, 51, 1229–1247. doi:10.1016/j.chb.2014.12.016

Guldentops, E. (2002). Governing Information Technology Through CobiT BT. *Integrity, Internal Control and Security in Information Systems: Connecting Governance and Technology*, 115–159. doi:10.1007/978-0-387-35583-2_8

- Hancock, D. R., & Algozzine, B. (2016). *Doing case study research: A practical guide for beginning researchers*. Teachers College Press.
- Heier, H., Borgman, H. P., & Mervyn, G. M. (2007). Examining the relationship between IT governance software and business value of IT: Evidence from four case studies. *Proceedings of the 40th Hawaii International Conference on System Sciences*.
- Hiererra, S. E. (2012). *Assessment of IT Governance Using COBIT 4.1 Framework Methodology: Case Study University IS Development in IT Directorate* (Masters Thesis). BINUS University, Jakarta, Indonesia.
- Huissoud, M. (2005). *IT self-assessment project, current results and next steps*. Presentation to EUROSAT IT Working Group, Cypress.
- Hunton, J. E., Bryant, S. M., & Bagranoff, N. A. (2004). *Core Concepts of Information Technology Auditing*. Wiley.
- Hyett, N., Kenny, A., & Dickson-Swift, V. (2014). Methodology or method? A critical review of qualitative case study reports. *International Journal of Qualitative Studies on Health and Well-being*, 9(1), 23606. doi:10.3402/qhw.v9.23606 PMID:24809980
- Information Security Governance. (2006). *Guidance for Boards of Directors and Executive Management*. Author.
- ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL: Information Systems Audit and Control Association.
- ISACA. (2013). *Self-assessment Guide: Using COBIT 5*. Rolling Meadows, IL: Information Systems Audit and Control Association.
- ITGI. (2003). *Board Briefing on IT Governance*. ITGI.
- Joshi, A., Bollen, L., Hassink, H., De Haes, S., & Van Grembergen, W. (2018). Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. *Information & Management*, 55(3), 368–380. doi:10.1016/j.im.2017.09.003
- Kaen, F. R. (2005). *Risk Management, Corporate Governance and the Public Corporation BT - Risk Management: Challenge and Opportunity*. Berlin: Springer Berlin Heidelberg. doi:10.1007/3-540-26993-2_21

- Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review*, 21(3), 243–255. doi:10.1016/j.hrmr.2010.07.001
- Lewis, S. (2015). Qualitative Inquiry and Research Design: Choosing Among Five Approaches. *Health Promotion Practice*, 16(4), 473–475. doi:10.1177/1524839915580941
- Lewis-Beck, M., Bryman, A. E., & Liao, T. F. (2003). *The SAGE Encyclopedia of Social Science Research Methods*. Thousand Oaks, CA: Sage Publications.
- Marrone, M., & Kolbe, L. M. (2011). Uncovering ITIL claims: IT executives' perception on benefits and Business-IT alignment. *Information Systems and e-Business Management*, 9(3), 363–380. doi:10.1007/10257-010-0131-7
- McEvoy, P., & Richards, D. (2006). A critical realist rationale for using a combination of quantitative and qualitative methods. *Journal of Research in Nursing*, 11(1), 66–78. doi:10.1177/1744987106060192
- McGuire, M. (2016). *The Impact of Performance Management on Performance in Public Organizations: A Meta-Analysis*. Academic Press. doi:10.1111/puar.12433.48
- McKay, J., Marshall, P., & Smith, L. (2003). Steps Towards Effective IT Governance: Strategic IT Planning, Evaluation and Benefits Management. *Pacific Asia Conference on Information Systems*, 956–970. Retrieved from <http://www.pacis-net.org/file/2003/papers/is-strategy/214.pdf>
- Moeller, R. R. (2011). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes* (2nd ed.). Hoboken, NJ: John Wiley & Sons. doi:10.1002/9781118269145
- Morse, J. M., & Niehaus, L. (2009). *Mixed method design: Principles and procedures* (4th ed.). Walnut Creek, CA: Left Coast Press.
- Nfuka, E., & Rusu, L. (2010). IT Governance Maturity in the Public Sector Organizations in a Developing Country: The Case of Tanzania. *AMCIS 2010 Proceedings*, 536.
- Nugroho, H. (2014). Conceptual model of IT governance for higher education based on COBIT 5 framework. *Journal of Theoretical and Applied Information Technology*, 60(2), 216–221.

Oliver, D., & Lainhart, J. (2012). COBIT 5: Adding Value Through Effective Geit. *EDPACS*, 46(3), 1–12. doi:10.1080/07366981.2012.706472

Pat, J. D., & Piattini, M. (2011). *Software Process Improvement and Capability Determination*. Academic Press. doi:10.1007/978-3-642-21233-8

Perry, C., Alizadeh, Y., & Riege, A. (1997). Qualitative methods in entrepreneurship research. *Proceedings of the Annual Conference of the Small Enterprise Association Australia and New Zealand*, 547–567.

Peterson, R. (2004). Crafting information technology governance. *Information Systems Management*, 21(4), 7–22. doi:10.1201/1078/44705.21.4.20040901/84183.2

Peterson, R., Parker, M., Ribbers, P., Peterson, R. R., & Parker, M. M. (2002). Information Technology Governance Processes Under Environmental Dynamism: Investigating Competing Theories of Decision Making and Knowledge Sharing. *ICIS 2002 Proceedings*, 562–575.

Peterson, R. R. (2001). Configurations and coordination for global information technology governance: Complex designs in a transnational european context. *Proceedings of the Hawaii International Conference on System Sciences*, 0(c), 217. 10.1109/HICSS.2001.927133

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 23(8), 638–646. doi:10.1016/j.cose.2004.10.006

Posthumus, S., Von Solms, R., & King, M. (2010). The board and IT governance : The what, who and how. *South African Journal of Business Management*, 41(3), 23–32.

Punch, K. F. (2013). *Introduction to Social Research: Quantitative and Qualitative Approaches* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Renaud, A., Walsh, I., & Kalika, M. (2016). Is SAM still alive? A bibliometric and interpretive mapping of the strategic alignment research field. *The Journal of Strategic Information Systems*, 25(2), 75–103. doi:10.1016/j.jsis.2016.01.002

Ribeiro, J., & Gomes, R. (2009). IT Governance using COBIT implemented in a High Public Educational Institution – A Case Study. *Proceedings of the 3rd International Conference on European Computing Conference*, 41–52.

Schubert, K. D. (2004). *CIO survival guide: The roles and responsibilities of the chief information officer*. Hoboken, NJ: John Wiley & Sons.

Selig, G. J. (2008). *Implementing IT Governance-A Practical Guide to Global Best Practices in IT Management*. Amersfoort, The Netherlands: Van Haren Publishing.

Siggelkow, N. (2007). Persuasion With Case Studies. *Academy of Management Journal*, 50(1), 20–24. doi:10.5465/amj.2007.24160882

Simonsson, M., & Johnson, P. (2006). Defining IT governance-a consolidation of literature. *The 18th conference on advanced information systems engineering*, 6.

Tonelli, A. O., de Souza Bermejo, P. H., Aparecida dos Santos, P., Zuppo, L., & Zambalde, A. L. (2017). It governance in the public sector: A conceptual model. *Information Systems Frontiers*, 19(3), 593–610. doi:10.1007/10796-015-9614-x

Turel, O., & Bart, C. (2014). Board-level IT governance and organizational performance. *European Journal of Information Systems*, 23(2), 223–239. doi:10.1057/ejis.2012.61

Van Grembergen, W. (Ed.). (2004). *Strategies for information technology governance*. IGI Global.

Wallhoff, J. (2004). *Combining ITIL with COBIT and ISO/IEC 17799:2000*. Scillani Information AB.

Warland, C., & Ridley, G. (2005). Awareness of IT Control Frameworks in an Australian State Government: A Qualitative Case Study. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 0(C), 236b–236b. 10.1109/HICSS.2005.116

Webb, P., Pollard, C., & Ridley, G. (2006). Attempting to define IT governance: Wisdom or folly? *Proceedings of the Annual Hawaii International Conference on System Sciences*, 8(C), 1–10. 10.1109/HICSS.2006.68

Weber, L. (2014). *Addressing the incremental risks associated with adopting a Bring Your Own Device program by using the COBIT 5 framework to identify keycontrols* (Doctoral Dissertation). Stellenbosch University.

Weill, P., & Ross, J. (2005). A Matrixed Approach to Designing IT Governance. *MIT Sloan Management Review*, 46(2), 26–34. doi:10.1177/0275074007310556

Wood, D. J. (2010). *Assessing IT Governance Maturity: The Case of San Marcos, Texas* (Masters Thesis). Texas State University, San Marcos, TX.

Section 3

Information Technology Agility in Large Organizations

Chapter 4

Strategic Agility

Frameworks for Information System Governance

ABSTRACT

In the current era, multiple factors have driven information systems (IS) to be able to cope with changes caused by internal and external factors that affect organization strategy. Various environmental factors can influence organization and performance capacity and tend to change organizational strategy, including political, socioeconomic, financial, and technological changes. Early in the 21st century, other changes are expected, such as those associated with cybercrime and artificial intelligence. Here, the authors discuss the concept of agility, the dimension of agility, relevant literature studies, and proposed model and conclusions.

INTRODUCTION

Today, the Department of Information Systems has more than ever the need to better manage their company's IT policy, which must not only make it possible to offer service availability or continuous business improvement, but above all offer competitive advantages linked to the use of information technology. In such a context, IT Departments must be based on the best approaches and practices to offer maximum agility to adapt to functional and technical evolutions and to open up in order to better connect to partners'

DOI: 10.4018/978-1-5225-7826-0.ch004

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

processes, while safeguarding and reusing existing IT assets without calling into question the technologies used for several years. Within this framework, a new type of information system, a natural evolution of current systems, will have to be defined and developed and which must be capable of being recycled over time, of being reconfigured effectively without generating new difficulties. In our opinion, this is an important opportunity to define and use a tool-based approach based on a rigorous methodological approach to guide architects and decision-makers in their process of development, redesign and modernization of corporate information systems.

To face the internal and/or external pressures that the company undergoes, control changes with the necessary responsiveness and reduce costs, so that the company ensures its survival, sustainability and security, it is vital to manage its information system with rigor and consistency, driving important and rapid changes at all levels of all dimensions of its information system. The changes concern technologies, applications, processes, organization and human resources. All these elements influence the company's strategy and vice versa. Thus, there must be sufficient agility in an information system so that it is aligned with the company's strategy.

However, the information systems deployed within companies are not always profitable and efficient, which can be explained by their lack of agility in an evolving environment, as well as by surprising changes, a situation in which their development is often forced, more than expected.

Today, the concept of agility is recognized as a means of maintaining consistency and improving the efficiency of IS. Therefore, the challenge is to keep information systems as open as possible while preserving the company's information assets; information systems must be able to respond quickly and effectively to changes.

Recently, the subject of IS agility has increasingly attracted the interest of IT researchers and practitioners. According to (Lee, Sambamurthy, Lim, & Wei, 2007; Sharifi & Zhang, 1999), the transformation of uncertainty in the business environment is a major topic of management research. The transformation of uncertainty requires that the important functions of any IS can cope with uncertainties.

In the current era, multiple factors have driven IS to be able to cope with changes caused by internal and external factors that affect the organization's strategy. Various environmental factors can influence organizational and performance capacity and tend to modify organizational strategy, including

political, socio-economic, financial and technological changes. At the beginning of the 21st century, other changes are expected, such as those associated with cybercrime and artificial intelligence. In this chapter, we discuss the concept of agility, the dimension of agility, relevant literature reviews and have proposed a conceptual model and conclusions.

LITERATURE REVIEW

Several authors in the past and more recently have given an immense interest on the agility concept (Sambamurthy et al. 2003; Overby et al. 2006; Rai et al. 2006; Tallon, 2008; Lu & Ramamurthy, 2011; Tallon & Pinsonneault, 2011; Nazir & Pinsonneault, 2012; Cai et al. 2013; Chen et al. 2014; Mao et al. 2014; Chen et al. 2015; Mao et al. 2015; Ragin-Skorecka, 2016).

At its main, agility entails the ability to react rapidly and flexibly to face change emerged from the technical domains and environment business. In addition, agility is defined as “the capacity of an interoperable system to detect its potential unsuitability versus environmental changes and to perform a relevant adaptation according to its component systems, in a reactive and effective manner (Zhang & Sharifi, 1999). In other words, we define agility as the ability to perceive, analyze and respond to changes in a turbulent environment based on competence, knowledge, and learning. In order to exploit and take advantage of the opportunities created by the changes (driver) of the environment based on the technical and organizational infrastructure. In Table 1, some popular definitions of organizational and IS agility are briefly presented.

The agility notion was introduced in the literature of organizational manufacturing strategic management at the beginning of the 90s, as a methodology to deal with the instability of the industrial environment and benefit from new opportunities produced through the environment changes to own a competitiveness.

How can firms become agile? How can they acquire the needed capacities? What exactly are these capacities?

Many researchers in the strategic and organizational management fields approached these questions, by referring to the theoretical works and theories preceding the initiation of agility concept. These theories and methods were adopted as a reference to Information Systems agility research.

As concerns, the agility concept was increasingly used in union with other terms such as the flexibility, the adaptability, and the reactivity. Inspired by

Strategic Agility Frameworks for Information System Governance

Table 1. Agility definitions

Authors	Definitions
(Goldman S. N., 1995)	For the company, agility means being capable of having a competitive advantage and continually predict the unpredictable requirements of customers.
(Zhang & Sharifi, 1999)	Agility means the capacity of an organization to detect, analyze and understand changes emerged by business environment, in the aim to face these changes (by changing its internal and external activities) and to perform appropriate solutions in fastest time.
(Helo, 2004)	Agility means a capacity of the organization to respond a change in a flexible way.
(Power D., 2005)	Agility means a combination between market knowledge and virtual corporation to take advantage of opportunities in a volatile marketplace.
(White, E.M, Daniel, & Mohdzain, 2005)	Supply chain managers must admit change but still need to improve a strategy that allows them to match supply and demand at an adequate cost. The capacity to accomplish this has been named supply chain agility. Information and more precisely agile information systems have been recognized as being a critical factor in achieving agility in the supply chain.
(Swafford, Ghosh, & Murthy, 2006)	An organization supply chain agility directly influences its capacity to create and deliver innovative products to their consumers in a brief time and cost with effective manner.
(Holmqvist & Pessi, 2006)	Agility permits to organizations to be able to sense and respond rapidly to unpredictable events and thus satisfy customer requirement changes. This capability is critical in today's business world. new technologies and the new manners of management of the business are constantly presented to create or change the global requests of the market.
(Lee, et al., 2006)	The company needs to address the specificities of the sites covering the activities of the global business. To meet these challenges, companies must have the capacity (that is agility) to develop and deploy quickly systems to answer to the emergent business needs.
(Desouza, 2007.)	Agility as a result of routines and quotidian practices that support strategizing between owners, senior management, and other important strategy processes participants, such as managers, consultants, and staff;
(Braunscheidel & Suresh, 2009)	An agility for supply chain is set as the company capability to more effectively collaborating with distribution partners to face market changes in a rapid manner.
(MITHAS, et al., 2011)	Postulate that knowledge management and agility are two important intermediaries that help implemented
(Yi, Ngai, & Moon, 2011)	Agility for the supply chain is considered as a crucial type of operational capability required for a high performance of the company.
(Kryvinska, 2012)	Agility supply chain is regarded as a crucial type of operational ability required for highly company performance
(Sørensen & Landau, 2015)	Defining academic agility as the ability of an academic field to examine quickly and ingeniously environmental changes in its main academic debate.
(Liu, Yang, Qu, & Liu, 2016)	Nowadays nearly all organizations count on information systems to operate. Agility in Information systems can be considered as critical to achieving overall agility in business.

the success of the agile methods in the field of the IT programming at the beginning of the 1990s, the practitioners interpreted the idea of the agile methods used in programming, an interpretation that still influences the adoption of the agility concept of many IT professionals.

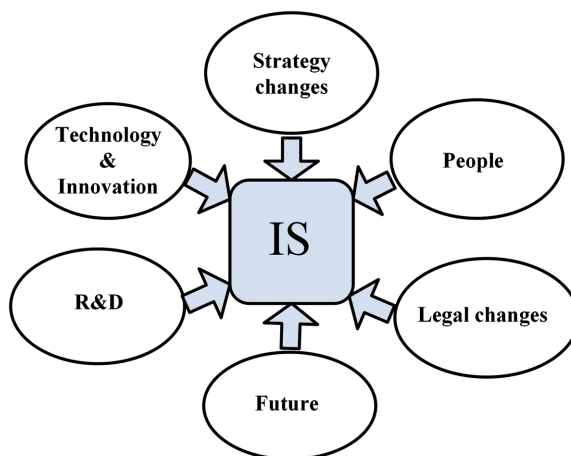
In the research literature, the concept of agility was attached to the way, which the system information reacted to face unpredictable changes such as the increase user's requirements, the process business changes, the strategic changes, the competitiveness, the organizational structure, the market changes, and the future changes.

In summary, various facets of agility were underlined by diverse authors which led to varied points of view, therefore the IS agility research was divided into several sub-domains such as (infrastructure, strategic IS, IT skills of IS professionals, governance of the IS, IS development methods, and software development). Though there is a difference in agility definition in the literature, these definitions are not opposite. However, the disadvantage is related to the lack of the global view of IS agility, lack of theoretical clarity, and conceptual parsimony in a different IS agile research areas, as shown in Figure 1.

LITERATURE METHODOLOGY

In our literature review, we adopted an exhaustive approach relative to the research objective. To achieve that, all appropriate and highly cited academic

Figure 1. Factors influencing information systems



publications are included in the examination process of our literature review based on several databases and research engines, such as (ProQuest, (Abi / inform), Elsevier, Emerald, Atypon, ACM digital library, ScienceDirect, IEEE Xplore, Gale Cengage computer), by using keywords as: “IS agility model, “agile IS”, “achieving agility in information systems”. The combination of used keywords depending on the review or the database. We viewed and treated identified articles; also, examined articles were identified through new citations and bibliographic references.

IS Agility Frameworks

Zhang and Sharifi, 1999

Because changes and the pressures on firms can be different, the agility level need by the manufacturing organizations will be also different. This level is cited with the term «the level of agility needed”, depending on various drivers such as the turbulence of the business environment, the company context, and the characteristics of the company, once “the necessary level of agility” is determined for the company, and the following step is to evaluate the agility level acquired by the organization. The difference between “the agility required level” and the level of agility that the company has already, is the level that the organization must meet in the order to be agile. The detection, recognition, and classification are the actions needed to identify different changes faced by the company, in the order to reduce a level of impact of each agility trigger individually. The level of agility capabilities required can be determined from the trigger of changes. In the final stage, a conceptual model comprises three steps: The first identifies agility providers that could bring about the required capabilities. The implementation of the identified providers is determined by the second step level of agility achieved (As a measure of performance), and in the third step, the formulation of corrective actions to further enhance performance is performed. Different tools must be developed to support firms with the aim to achieve an overhead process that has already cited.

In summarizing, the researchers (Zhang & Sharifi, 1999) have proposed a methodology to detect a different change in the business environment, in which the company must have the ability to determine the desired agility level. The strategies available to the company in the aim to determining the unpredictable changes, which influences its strategy and sometimes even

threaten its existence and define the capabilities and priorities in order to implement the capabilities needed by the firm to faced changes and identify the ways that could support the company to intercept change. The model proposed by Zhang and Sharifi (1999) is presented in Figure 2.

Gunasekaran and Y. Yusuf, 2002

The researchers (Gunasekaran & Yusuf, 2002) have developed their agility management (AM) adequate to firms that work in an aerospace industrial firm context. This survey evaluated the company’s agility by taking a technical study with the assistance of a suitable questionnaire. The objective is to revise agility prospects in the manufacturing sector to identify key AM strategies and technologies. In addition, the authors have proposed a framework to become agile for Industrial Systems Based on four key: strategy, people, technology, and systems as shown in Figure 3.

Crocitto and Youssef, 2003

The authors (Crocitto & Youssef, 2003) consider organizational agility (OA) as the combination of organizational processes, characteristics, and people with advanced technology. Agility improves the Capability of the organization

Figure 2. A methodology for achieving agility in manufacturing organizations (Zhang & Sharifi, 1999)

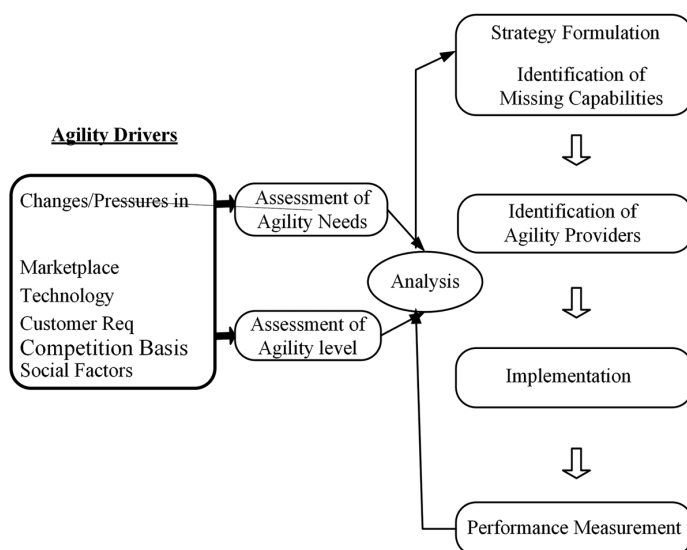
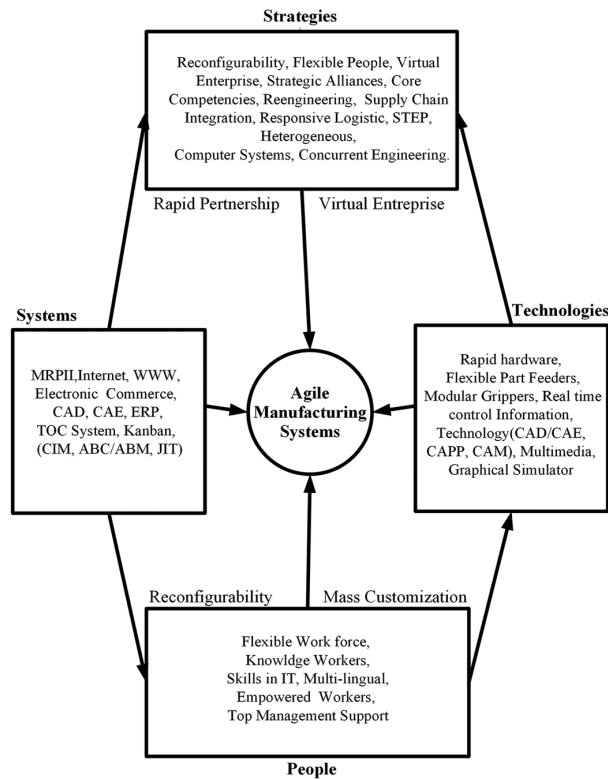


Figure 3. Methodology to achieve agility in manufacturing systems (Gunasekaran & Yusuf, 2002)

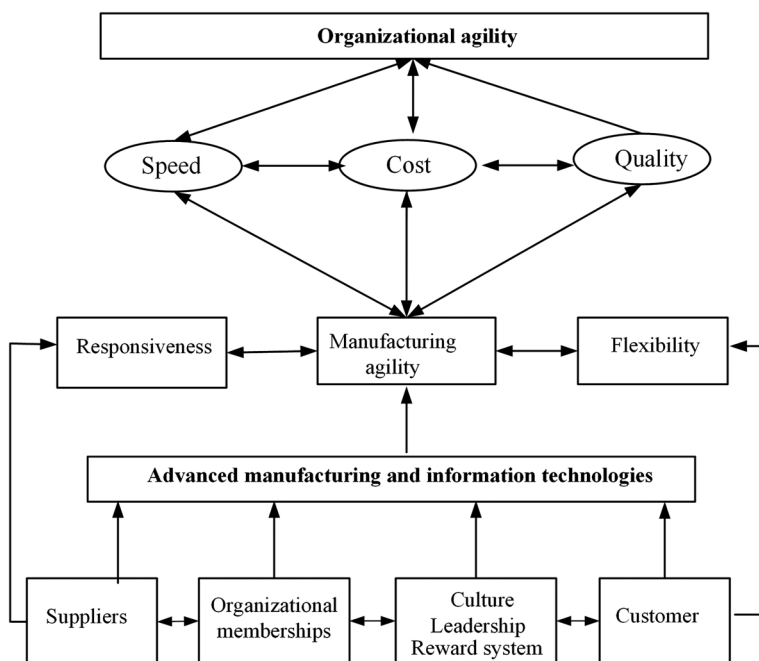


to provide products and services with high quality with the aim to increase an organizational competitiveness.

They propose an integrated production/operations, general management, and socio-technical opinions in order to develop a model of OA. The proposed model is based on agile suppliers, members of the organization and united customers through information technology. It is suggested that these connections are based on a basic leadership, a culture of the organization and employee reward systems that create a relationship between technology and people.

These relationships include the involvement of people in the process of decision-making, the creation process and product with high quality, by proposing enhanced jobs, technological training, and reward system that increases the organizational agility level.

Figure 4. Model of organizational agility (Crocitto & Youssef, 2003)

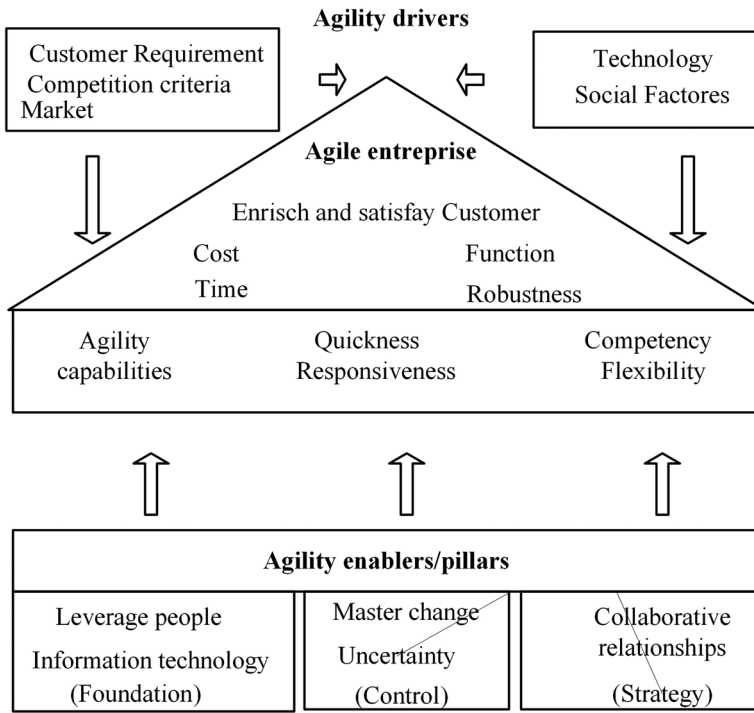


In summary, the authors propose a model based on the integration of the human element to achieve OA and get a competitive advantage as shown in Figure 4.

Lin, Chiu, and Tseng, 2006

The aim of the agile organization is to enhance/satisfy employees and clients. Change is the principal cause behind agility. Even though, change is nothing new, today's change is taking place at a much quicker speed than ever earlier. Turbulence and unpredictability in the market environment have become the principal reasons for failure in the manufacturing industry. In short, the number of changes and their type, specification or feature, cannot be readily shaped and are probably indefinite. Therefore, the authors (Lin, Chiu, & Tseng, 2006) have evolved a model containing four aspects to be agile. The first prospect is that customer requirement, competition criteria, market, technology, and social factors are changing competition in business environments (Agility drivers). In the second aspect, the agile organization tries to enrich and satisfy customers based on components such as cost, time,

Figure 5. A conceptual model for the agile enterprise (Lin, Chiu, & Tseng, 2006)



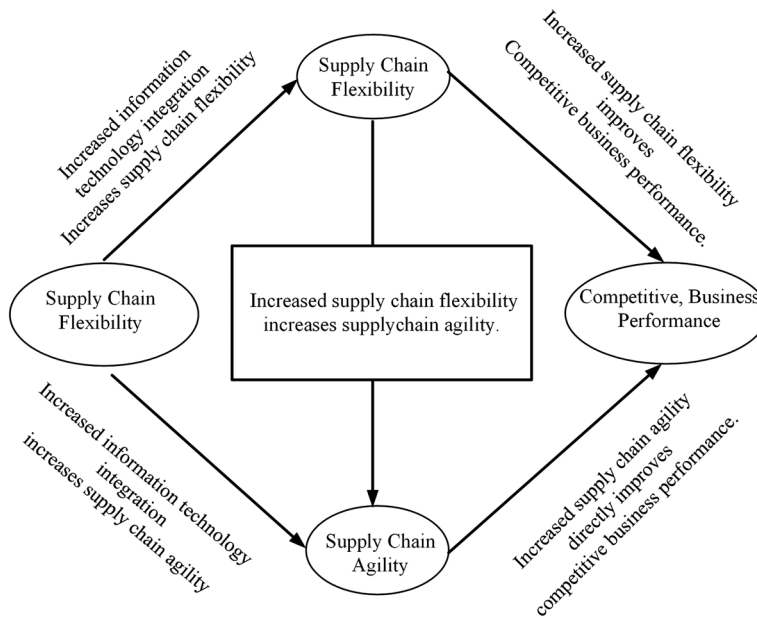
purpose, and hardiness. Agility capabilities involved in the third facet are flexibility, responsiveness, quickness, and competency. The proposed model is presented in Figure 5.

Swafford, Ghosh, and Murthy, 2008

The authors proposed a process based on a framework of agility in an organization's supply chain. Three key factors that define the flexibility of the attributes of three fundamental processes of the supply chain in a firm of logistics or distribution, procurement or sourcing and manufacturing are presented in their framework.

In addition, they emphasized the factors that constitute the history of its supply chain agility, they also develop the structures and assumptions for the supply chain agility as presented in Figure 6.

Figure 6. A conceptual model for an agile enterprise (Swafford, Ghosh, & Murthy, 2008)



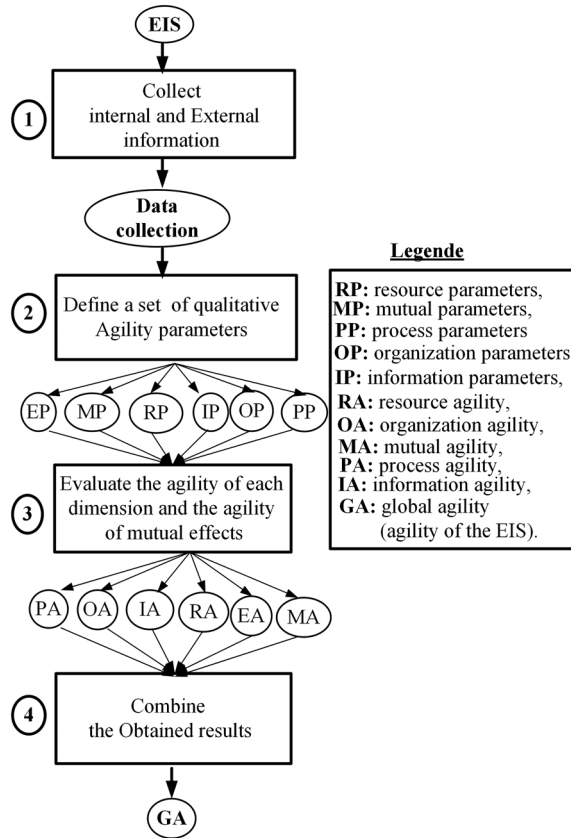
Ramesh, Mohan, and Cao, 2012

According to (Ramesh, Mohan, & Cao, 2012) the strategy of the company is influenced by different elements like environment, socioeconomic, legislative, technological, and globalization changes. That increases the complexity of its information system and the ferocity of competition. For a company to be sure of its position in a context characterized by a rapid and a random change in external environments, it must have a fast adaptation policy, a strategy to rapidly make important changes for all systems to align it with its strategy and conversely; which means, it must always be agile. Therefore, to achieve enterprise agility, it is necessary to consider the information system agility as an objective.

In their papers, the researchers discuss the assessment of agility in the POIRE (Process, Organization, Information, Resource, and Environment). Others propose an evaluation approach based on fuzzy logic with the aim to continuously measure, regulate and agility of the system. It also proposes a prototype applying the proposed approach to a tour operator company.

According to the authors, first of all, we must define the target IS, which will best serve the company’s strategy, and satisfy the business process, in

Figure 7. POIRE agility evaluation approach (Ramesh, Mohan, & Cao, 2012)



short an aligned information system; Second, to lay down construction rules that allow the system to avoid repeating gaps in the old information system and anticipate changes, in short an Agile IS. Finally, determining the trajectory transformation from the present IS to the target IS, it needs to emphasize the current information system in order to define appropriate criteria for achieving the restructuring phase. This model is presented in Figure 7.

DISCUSSION AND CRITICS

Discussion

The IS Agility has attracted the attention of researchers since the 1990s with articles proposing many approaches and concepts for organizations and their information systems in order to respond off the new requirements of organizations, information systems, employees and customers.

At the beginning of the 21st century, agility research has evolved from the general explanation of the agility paradigm to the explanation of agility through the attributes of the computer system, the development methods and practices of outsourcing, and the (IS) staff. Research on IS agility was therefore divided into different sub-areas such as (Strategic IS Management, Business agility and the value of IS applications, IT Infrastructure, Skills of IS Professionals, Governance of the IS, Methods used in IS development, Methods used in Software Development) which gives a diversity in research presented to date.

The strategic agility of IS presents a severe challenge for researchers. The agility notion still not clearly defined and conceived. Although the primary and the principal drivers of agility such as (People, R&D, Legal changes, Strategy changes, technology change, Future changes) have been cited in the literature review.

Nowadays, the above agility requirement constitutes a major preoccupation of organizations, which seeks more flexibility and Reactivity to cope with diverse changes. In other words, SI must have the capacity to modify its structure, after a pertinent analysis of the existing IS, and their requirements.

Critics

We do not find a general definition of agility; there are various opinions about the meaning of agility concept. In research, the term of agility is used to define the way that (IS) can be adapted to cope with the unpredictable change emerging from internal or external the organization.

No one of the above models have cited an IS security, such as a driver for agility. In addition, the proposed models and methodologies do not get up any systemic process for the implementation of agility except (Zhang & Sharifi, 1999). In addition, the proposed models are essentially based on manufacturing area and do not give a holistic and comprehensive approach

to agility measurement and improvement in another organizational context, such as (the organization operating in the public or service sectors.).

These models proposed a methodology for enhancement of flexibility, but no one of them suggests a practical method for agility assessment and improvement.

THE AGILITY COMPONENTS

As you saw in the literature section one of the most interpretations to define the agility concept is “the capacity to adapt to changes” (Conboy, 2009). Information technology is thought to be an essential ability for increasing organizational agility (Woodard, Ramasubbu, Narayan, Tschang, & Sambamurthy, 2013). According to Lu and Ramamurthy (2013), IS agility is generally considered as an enabler of a firm’s agility. Acknowledges that, which IT capability as an underlying component reflected in three dimensions:

- IT infrastructure capability (the technological foundation),
- IT business capability (business-IT strategic thinking and partnership),
- IT proactive stance (opportunity orientation). In this perspective, IS must first identify agility drivers to determine the required level of IS agility. To define the current level of IS agility we must identify the agility providers. This latter helps IS to improve their existing capabilities and specify the capabilities to promote the ability to face changes.

Agility Drivers

According to Markus and Robey (1988) conceptual models are generally derived from process theories or variance (factor); also, researchers have cited several factors about drivers, capabilities, and providers.

Drivers

According to Zhang (1999), the drivers of agility are the changes/pressures emerging from the business environment, which are necessities for a company to find new solutions in order to maintain its competitiveness. In addition, Susarla et al (2012) argue that new emerging operational priorities require

Table 2. Agility drivers types

Type	Drivers	Authors
Technology	IT architecture, Planning and development, The introduction of new technologies.	(Zhang & Sharifi, 1999) (Felipe, Roldán, & LealRodríguez, 2016) (Fink & Neumann, 2007) (Schmidt & Buxmann, 2011) (Joachim, Beimborn, & Weitzel, 2013)
Strategy	Business value (IT investments), Assessment framework, Analysis and planning, Governance, Migration planning, Development, Managing strategic changes.	(Overby, Bharadwaj, & Sambaurthy, 2006)
People	Client satisfaction Personnel skills and competencies. Customer requirement. Interpersonal and management skills.	(Avital, et al., 2006)
Security	Attacks Vulnerability Incidents Intrusions. Breaches,	(Kankanhalli, Teo, Tan, & Wei, 2003) (Pereira & Santos, 2010) (Soares & Sá-Soares, 2014) (Polónia & de Sá-Soares, 2013)
R&D	Best practices Management IS Work process Rules	(Weill, Subramani, & Broadbent, 2002) (Hugoson, Magoulas, & Pessi, 2008) (Zheng, Venters, & Cornford, 2011) (Wang, Conboy, & Cawley, 2012)
Organization environment	Competitors' actions Economic shifts	(Sambamurthy, Bharadwaj, & Grover, 2003) (Overby, Bharadwaj, & Sambaurthy, 2006)
Legal	Regulatory/legal changes	(Overby, Bharadwaj, & Sambaurthy, 2006)

new IS capabilities. In Table 2, we have listed seven different categories of drivers change relevant to information systems: Strategy, Technology, Legal changes, People organizational, Security and finally Research and development (R&D).

Capability

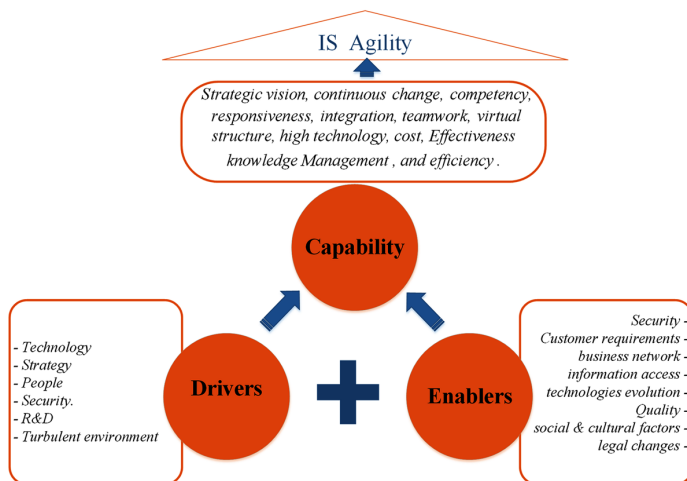
The literature has indicated tree type of IS capability:

- **Technical Capability:** Refers not only to the specific technical specialties (including programming, understanding software

development processes and knowledge of operating systems, database systems, and other such areas), but is also concerned with the understanding of where and how to deploy IT effectively in order to support the strategic goals and objectives of an organization (Lee et al., 2006). IT personnel with a solid technical capability are more likely to provide effective technical solutions faster.

- **Business Capability:** Relates to the ability of IT personnel to comprehend the business processes they support as well as the organizational consequences associated with the practical solutions they implement. Such ability requires general business knowledge, organization-specific knowledge, and knowledge to learn about business functions (Lee, et al., 2006; Byrd, Pitts, Adrian, & Davidson, 2008; Fink & Neumann, 2007)
- **Personnel Capability:** Means a set of interpersonal and management knowledge and skills which are especially critical to IT personnel who habitually assume a boundary spanning role in their organizations (McCann, Selsky, & Lee, 2009). Such capability includes project management, team collaboration, planning, presentation and communication, organizing and leading projects etc. (Fink & Neumann, 2007); IT personnel with strong behavioral capability are often sensitive to organizational culture and politics, which makes them, work efficiently and effectively across business functions.

Figure 8. Agility researches components



Researchers suggest three main phases to agility. Those are agility drivers, agility's capabilities, and agility enablers or providers. Several factors have been emphasized on the capacities of drivers and enablers in the IS fields. Here, we combine those elements to form a new and complete model of organizational agility areas. Figure 8 describes (the different component to achieve agility).

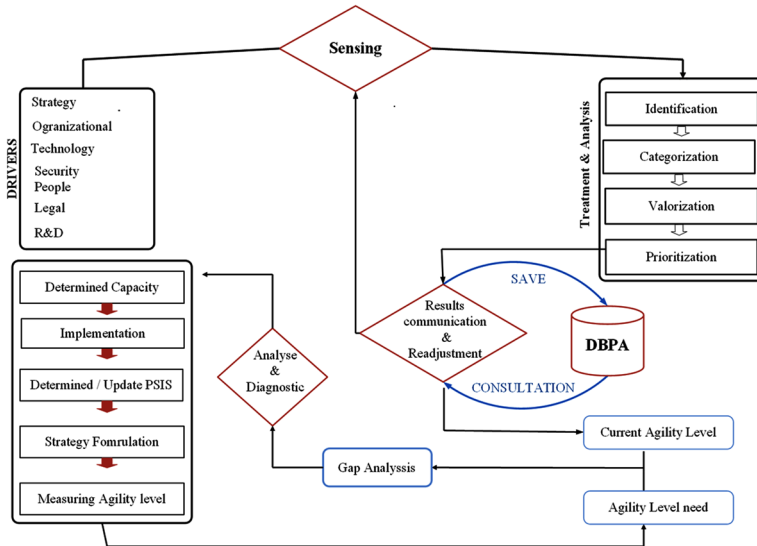
THE PROPOSED CONCEPTUAL MODEL TO ACHIEVE STRATEGIC AGILITY

In Figure 9, we proposed a model for a practical methodology of IS strategic agility. Founded on this model, any IS requires to examine external and internal IS environment. At the first step IS must sensing diverse internal and external drivers. These factors represent the organizational strategy, technology, people, legal changes, intra-organizational context, technology, security, R&D, organizational environment, and so on. At the second stage, it is important to identify the drivers that press on IS to change or challenge the IS life and survive. Therefore, is need to resolve rapidly and efficiently agility's drivers as they meet with those factors. This would require the identification, categorization, valorization, and prioritization of changes faced by the company, as well as the analysis of the impact individual changes will bring to the company.

The results of this and previous stage can be analyzed in the order to determine the strong and weak point. At this position is should determine an agility level needed to react with an efficient way to the changes or pressures. The IS needed agility level is considered equivalent to the degree of drivers change impact. The difference between the required level of agility and the existing, constitute a supplementary pillar of decision-making after its analysis. In this work, the results of the examination are typically classified into four types:

- The IS does not need to respond;
- The (IS) agility level is satisfactory to answer to changes as might be encountered in the future;
- The (IS) must be agile but not in an emergency;
- The IS must be agile effectively and urgently.

Figure 9. A conceptual model to achieve IS agility



The next step following the measuring of needs agility is to define the requisite agility capabilities in aim to become agile. The last stage of the model requires determining the agility Drivers, which could provide the necessary capabilities, implement the identified providers, determine the current agility level, and finally formulate corrective actions in order to enhance performance. It should be noted that a number of tools must be developed to support properly carry out the above model.

Sensing

Recall that the relevant forces of environmental change include competitor actions, strategic changes, and changes in consumer preferences or IS staff skills, economic changes, regulatory and legal changes, and technological advances. These different changes require a standby to detect any potential changes regarding each of these types.

For example, an organization needs the capacity to sense market changes, track competitors' actions, consumer preferences change and economic changes. Furthermore, sensing regulatory and legal changes that have an impact on a company's is a necessity and this through government relations department or legal service... Finally, effective research, development, and IT capabilities will be required to detect technological progress and the ways

in which an organization can exploit them with the aim to take competitive advantage.

According to Brynjolfsson and Mendelson (1993), the information system is the core of the company. Viewing its role, the IS must have a strategic intelligence sensing on all elements influencing the company and its strategy. According to Brynjolfsson and Mendelson (1993), the information system is the company core. Viewing its role IS must have a sensing on all elements influencing the company and its strategy. Today an important flow of information requires a daily listening on Aggregators, alerts, RSS feeds, networks social, ERP, and so on, with the aim to detect an opportunity or anticipate a menace. The Table 3 illustrates the types of sensing which organization can adopt.

- Scientific sensing, which covers all areas that could give the company a competitive advantage based on scientific evolution (science, technology, processes, and methods);
- Societal sensing, this sensing consists of discerning among a certain number of changes “demographic evolution, cultural changes, ...” the great changes which are taking place in society and which risk transforming or disrupting the company and its environment. Through the study of cultural, political, social and historical factors, institutional, political actors (state, administrations, local authorities, trade unions), public opinion, the evolution of regulations and the environment.
- Commercial and competitive sensing, which includes the business aspects (centered on markets, customers, business methods, etc.) And competitive (about competitors and new entrants, products, and especially new alternative products, Relations with suppliers, consumer relations, etc.);
- The strategic sensing, which benefits from the coordination of the various existing watch structures. Another way to segment the various forms of what is to distinguish them according to their time horizons, their fields of application and the nature of the actors required: sensing is a “continuous and largely activity to sense a different change driver such as the technological societal, commercial and competitive environment. That is mean permit an organization to anticipate changes».
- Social media sensing: Nowadays, Social Media sensing has become a necessity for any companies wants to plan and manage their communication on social networks or keep an eye on competitors.

Table 3. Sensing types

Sensing types	Temporal Horizon	Target	Actors
Scientific	Permanent long-term	Scientific database Scientific congress Journals and Scientific reviews.	Department of Prospective. Department Strategy. R&D
Societal	Permanent long term	Political actors. Study of cultural, political, social and historical factors. Public opinion	Department of perspective. Department strategy. R&D. Product Manager Division of Product.
Commercial and competitive	Permanent Short Term	Analysis of competitive movements. Alternatively, the introduction of new products. - Analysis of a Market event.	Responsible Operational Divisions
Strategic sensing	Short Terms	Detection of incongruities; Conferences, fairs, Symposiums.)	Top management Agility team
Social media Sensing	Permanent long-term	Analyze information on current topics related to their companies	Marketing managers

Marketing managers can analyze information on current topics related to their company. In addition, it is possible to monitor exchanges of opinions, discussions, and trends in real time. The Social Media monitoring allows having a vision on the influencing Web exchanges. Also, identify and react in real-time to the critics.

To describe and specify the subjects that interest the organization and for which it is required to collect data or information it is necessary to define the sensing axes and the purposes that should concern the strategic factor, commercial, competitive, technological, legal, regulatory, economic, societal, etc. On the other hand, to identify the objectives targeted by the decision-makers, that means, the strategic objectives of the company.

In the stage of identification and selection of information sources, among the various existing sources (such as Big-Data, databases, documentation centers, experts or specialists, periodical publications, books, professional events, actors in the field, social networks, etc.).

To choose the relevant sources and accessible according to their specific characteristics, the sensing axes and the types of information required, constraints imposed by the company on delays, confidentiality and costs.

The sensing phase must carry out on a regular or variable data sources, giving the right level of pertinence to the information corresponding directly or indirectly to the sensing axes.

In the phase of identifying, processing and analyzing the collected data, it is a question of analyzing the collected information and organizing it in such a way as to make it exploitable.

Finally, the phase of validation and readjustment after communication of the results allowed the adjustment by deepening or reorientation of the objectives and means of sensing as shown in Figure 10.

DBPA

DBPA (Agility Data Base Provider) will allow managing agility providers for each organization and key information. The establishment of a reference is necessary to improve the level of agility of the SI and to be able to exploit it in the future.

By centralizing the various information available after the communication phase of the results, this will make it possible to manage all the characteristics of all the providers managed and listened. Building a database is necessary to improve agility. In an approach based on the results communicated and the relevance of the information. The DBPA will allow managing all the characteristics on all the agility triggers that press on the IS as:

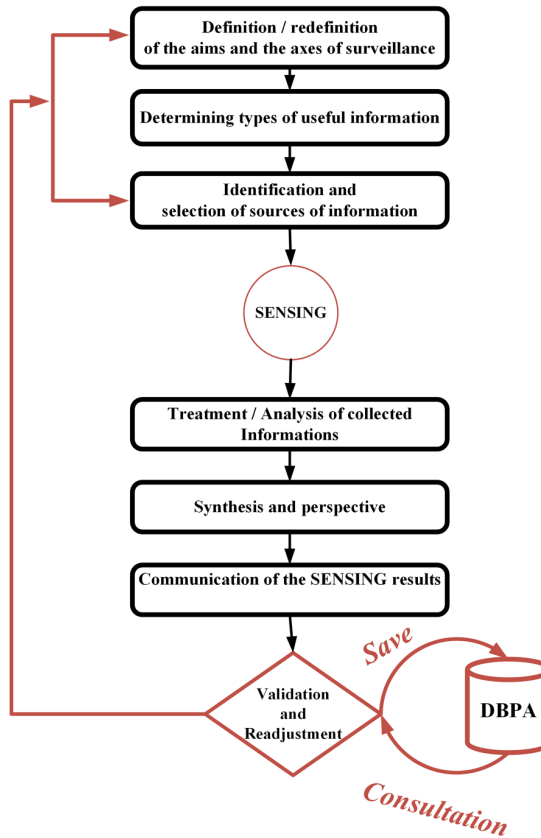
- Identification of the configuration items CIs and attributes associated with each provider,
- Complete history of all activities related to a provider,
- Intuitive modeling of relationships between provider,
- Impact analysis on IS, on users,
- Possible solutions and actions.

The Level of Agility Need

Assess the level of agility needed is important with the aim to determine the contexts in which agility is necessities and those in which agility may represent wasteful of resources.

We estimate that environmental conditions become increasingly turbulent for firms across success, organization agility will be important for firm

Figure 10. SENSING phase



success. The needed agility level for an IS considered equal to the level of IS internal and external changes.

Assessment of Current Agility Level

To evaluate a current IS agility, it is necessary to consider the change generated by factors being marked in the model include general actors such as Strategy, Technology, people, R&D, Security, organization environment. The IS must sense proactively needs organization and its external environment and take advantage of unexpected opportunities. Because each of these general factors is divided into some sub-factors, the evaluation tool should also take structure layers. A top layer corresponds to the general areas to be evaluated

and a second layer corresponds or specific agility driver each information systems and organization.

Security Policy

When an organization decides to make a change in its information systems. A security assessment related to this change becomes a necessity otherwise an obligation, in order to study each possible vulnerability, this evaluation must include an explicit analysis of the security policy and the existing procedures; Emphasize should be placed on detecting vulnerabilities that may or may not be used to infiltrate or get data.

Ideally, we should start by defining a comprehensive cybersecurity strategy and/or a cyber-risk assessment. These will give an important starting point. Failing that, we should consider the cyber standards of security that the organization must adopt, such as: risks, and contractual relationships that we must respect.

We must ensure a conformity of the security policy with the standards of IS security, we need essentially write completely new security policies which are determined by new requirements (new capacity).

Maintain accurate registers of system files, Software, hardware problems, and service requirements. Good knowledge and support of the technologies and elements to be introduced to the IS. Maintain efficient support for the end-user support process, back-office, and a backup for any application in IS.

It should be noted that it is essential to reach a solid agreement with the Top management of the organizations. Otherwise, this will be the first obstacle to non-compliance with the new policy thing that will certainly affect the security level of the organization.

The Proposed Model Contribution

As you know, the purpose of this chapter is to provide a conceptual model for assessing and enhancing IS agility in order to respond effectively to any internal and external changes in the organization.

None of the models or methodologies previously described in the literature propose a systematic model for the implementation of agility except Zhang (Zhang & Sharifi, 1999). Although these models designate three parts of agility as drivers, capacities, and enablers, but do not agree on the elements of these fundamental parts. In addition, many steps such as the strategy

formulation, the external and internal environmental evaluation, the agility measurement process and the development of action plans are not clearly identified and articulated.

As you have seen in the agility's approach section, the authors have set out many different definitions for the agility concept but they not agree on a unique definition. We define agility as the ability to cope with driver changes by using enablers in order to gain beneficial capabilities.

In summary, the main characteristics of this methodology than previous models are:

- The proposed model has a systematic approach to guides information systems direction to implement agility easily and successfully;
- Internal and external drivers of change are considered and determined in this model;
- Many factors, capabilities, and providers have been identified in this model;
- Strategy formulation and action plans are mentioned in order to move away from the traditional IS to the Agile IS;
- Provide many approaches to measure a level of agility that IS has gained to re-analysis conditions and design improvement initiatives;
- A security policy for IS (PSIS) formulation or an update in the case of existing PSIS must be applied in order to consider the new changes and preserve the information patrimony;
- Some agility frameworks make an attempt to present a more integrated and holistic model still has a vision mainly centered on production and technological aspects of the company, but, this model can be applied to any organization (whether profit, nonprofit, service, public and private);
- This model shows the need for a knowledge-based system for further distinguished the new changes;

Finally, a method to measure agility must be adopted and applied frequently maintain the synergies of IS and Agility level, with the aim to intercept the changes evolving from inside and/or outside the organization.

CONCLUSION AND FUTURE WORK

From a strategic point of view, agility lies in the conquest of new markets, in risk-taking, in the apprehension of new social and environmental issues. Thus, at the level of the operational strategy, it consists of an ability to integrate the stakeholders into the business practices and a better understanding of the business by re-estimating all the links of the chain of value in a logic of creating a competitive advantage. In other words, talking about agility is necessarily about strategy and, more specifically, about the organization, culture and management model that will make it possible to best relay the need for reactivity.

This chapter introduced the concept of agility in enterprise information systems and the frameworks for producing and evaluating agility. Although these frameworks are relevant, they are still at the conceptual stage and therefore of limited scope and maturity. Being able to define new and/or improve existing ones, methodologies and integrated tools allowing the concept of agility to be taken into account throughout the life cycle of the information system would be a considerable contribution for companies which must find effective means enabling them to survive and evolve serenely within the current economic environment characterized by fierce competition and rapid and random changes.

For future work, we will concretely measure the proposed model assessing and controlling the agility of organizations in order to better manage agility and ensure its evolution with serenity while basing itself on the concepts of urbanization, continuous improvement, flexibility, integration and interoperability, in the context of globalization and unpredictable changes in contingency variables.

The next chapter addresses the topic of agility for IT service management. It will propose a practical framework to address this issue.

REFERENCES

Allen, B., & Boynton, R. (1991). Information Architecture: In Search of Efficient Flexibility. *MIS Quarterly*.

- Avital, M., Lyytinen, K. J., Boland, R., Jr., Butler, B. S., Dougherty, D., Fineout, M., . . . Venable, J. (2006). Design with a Positive Lens: An Affirmative Approach to Designing Information and Organizations. *Communications of the Association for Information Systems, 18*(1). Retrieved from aisel.aisnet.org/cais/vol18/iss1/25
- Baskerville, R., & Pries-Heje, J. (2004). Short cycle time systems development. *Information Systems Journal, 14*(3), 237–264. doi:10.1111/j.1365-2575.2004.00171.x
- Benamati, J., & Lederer, A. (2001). Coping with Rapid Changes in IT. *Communications of the ACM, 44*(8), 83–88. doi:10.1145/381641.381664
- Bhatt, G., Emdad, A., Roberts, N., & Grover, V. (2010). Building and leveraging information in dynamic environments: The role of IT infrastructure flexibility as enabler of organizational responsiveness and competitive advantage. *Information & Management, 47*(7–8), 341–349. doi:10.1016/j.im.2010.08.001
- Boar, B. (1998). Redesigning the IT Organization for the Information Age. *Information Systems Management, 15*(3), 23–30. doi:10.1201/1078/43185.15.3.19980601/31131.4
- Börjesson, A., Martinsson, F., & Timmerås, M. (2006). Agile Improvement Practices in Software Organizations. *European Journal of Information Systems, 15*(2), 169–182. doi:10.1057/palgrave.ejis.3000603
- Braunscheidel, M. J., & Suresh, N. C. (2009). The organizational antecedents of a firm's supply chain agility for risk mitigation and response. *Journal of Operations Management, 27*(2), 119–140. doi:10.1016/j.jom.2008.09.006
- Broadbent, M., Weill, P., & St.Clair, D. (1999). The Implications of Information Technology Infrastructure for Business Process Redesign. *Management Information Systems Quarterly, 23*(2), 159–182. doi:10.2307/249750
- Brynjolfsson, E., & Mendelson, H. (1993). Information systems and the organization of modern enterprise. *Journal of Organizational Computing and Electronic Commerce, 3*(3), 245–255. doi:10.1080/10919399309540203
- Butler, B., & Gray, P. (2006). Reliability, Mindfulness, and Information Systems. *Management Information Systems Quarterly, 30*(2), 211–224. doi:10.2307/25148728

- Byrd, T., & Turner, D. (2000). Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct. *Journal of Management Information Systems*, 17(1), 167–208. doi:10.1080/07421222.2000.11045632
- Byrd, T. A., Pitts, J. P., Adrian, A. M., & Davidson, N. W. (2008). Examination of a path model relating information technology infrastructure with firm performance. *Journal of Business Logistics*, 29(2), 161–187. doi:10.1002/j.2158-1592.2008.tb00091.x
- Celen, M., & Djurdjanovic, D. (2012). Operation-dependent maintenance scheduling in flexible manufacturing systems. *CIRP Journal of Manufacturing Science and Technology*, 5(4), 296–308. doi:10.1016/j.cirpj.2012.09.005
- Ciborra, C. (1992). From Thinking to tinkering: The grassroots of IT and strategy. *The Information Society*, 8, 297–309. doi:10.1080/01972243.1992.9960124
- Clark, C., Cavanaugh, N., Brown, C., & Sambamurthy, V. (1997). Building Change-Readiness Capabilities in the IS Organization: Insights From the Bell Atlantic Experience. *Management Information Systems Quarterly*, 21(4), 425–455. doi:10.2307/249722
- Conboy, K. (2009). Agility from first principles: Reconstructing the concept of agility in information systems development. *Information Systems Research*, 20(3), 329–354. doi:10.1287/isre.1090.0236
- Crocitto, M., & Youssef, M. (2003). The human side of organizational agility. *Industrial Management & Data Systems*, 103(6), 388–397. doi:10.1108/02635570310479963
- Desouza, K. (2007). *Agile information systems: Conceptualization, Construction and Management*. Butterworth-Heinemann.
- Drucker, P. (1968, April). *Comeback of the entrepreneur*. Academic Press.
- Duncan, N. (1995). Capturing Flexibility of Information Technology Infrastructure: A Study of Resource Characteristics and Their Measure. *Journal of Management Information Systems*, 12(2), 37–57. doi:10.1080/07421222.1995.11518080
- Dybå, T., & Dingsøy, T. (2008). Empirical Studies of Agile Software Development. *Systematic Reviews*, 50(9–10), 833–859.

- Felipe, C. M., Roldán, J. L., & Leal-Rodríguez, A. L. (2016). An explanatory and predictive model for organizational agility. *Journal of Business Research*, 69(10), 4624–4631. doi:10.1016/j.jbusres.2016.04.014
- Fink, L., & Neumann, S. (2007). Gaining agility through IT personnel capabilities: The mediating role of IT infrastructure capabilities. *Journal of the Association for Information Systems*, 8(8), 440–462. doi:10.17705/1jais.00135
- G., B., A., E., N., R., & V, G. (2010). Building and leveraging information in dynamic environments: The role of IT infrastructure flexibility as enabler of organizational responsiveness and competitive advantage. *Information and Management*, 47(7–8), 341–349.
- Gebauer, J., & Schober, F. (2008). Information system flexibility and the cost efficiency of businessProcesses1. *Journal of the Association for Information Systems*, 7(3), 122–146. doi:10.17705/1jais.00084
- Gebauer, J. L. F., & Lee, F. (2008). Enterprise System Flexibility and Implementation Strategies: Aligning Theory with Evidence from a Case Study. *Information Systems Management*, 25(1), 71–82. doi:10.1080/10580530701777198
- Gerth, A. R., & Rothman, S. (2007). The Future IS Organization in a Flat World. *Information Systems Management*, 24(2), 103–111. doi:10.1080/10580530701221007
- Goldman, S., & Nagel, R. (1993). Management, technology and agility: The emergence of a new era in manufacturing. *International Journal of Technology Management*, 8(1/2), 18–38.
- Goldman, S. N. (1995). *Agile Competitors and Virtual Organizations: Strategies for Enriching the Customer*. New York: Van Nostrand Reinhold.
- Gunasekaran, & Yusuf, Y. (2002). Agile manufacturing: A taxonomy of strategic and technological imperatives. *International Journal of Production Research*, 40(6), 1357–1385. doi:10.1080/00207540110118370
- H, T., R, A., & N, V. (2010). Research Commentary: Reframing the Dominant Quests of IS Strategy Research for Complex Adaptive Business Systems. *Information Systems Research*, 214, 822–834.
- Helo. (2004). Managing agility and productivity in the electronics industry Petri. *Industrial Management and Data Systems*, 104(7), 567. doi:10.1108/02635570410550232

Holmqvist, M., & Pess, K. (2006). Agility through scenario development and continuous implementation: A global aftermarket logistics case. *European Journal of Information Systems*, 15(2), 146–158. doi:10.1057/palgrave.ejis.3000602

Hong, W., Thong, J. Y., Chasalow, L. C., & Dhillon, G. (2011). User acceptance of agile information systems: A model and empirical test. *Journal of Management Information Systems*, 28(1), 235–272. doi:10.2753/MIS0742-1222280108

Hugoson, M.-Å., Magoulas, T., & Pessi, K. (2008). Interoperability Strategies for Business Agility. *Advances in enterprise engineering*, 108-121. doi:10.1007/978-3-540-68644-6_8

J, R., & Fliedner, V. G. (1998). The journey toward agility. *Industrial Management & Data Systems*, 48(9), 165 – 171.

J., R., Vokurka, & Fliedner, G. (1998). The journey toward agility. *Industrial Management & Data Systems*, 98(4), 165-171.

Joachim, N., Beimborn, D., & Weitzel, T. (2013). The influence of SOA governance mechanisms on IT flexibility and service reuse. *The Journal of Strategic Information Systems*, 22(1), 86–101. doi:10.1016/j.jsis.2012.10.003

Kankanhalli, A., Teo, H., Tan, B., & Wei, K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 32(2), 139–154. doi:10.1016/S0268-4012(02)00105-6

Kryvinska, N. (2012). *Building consistent formal specification for the service enterprise agility foundation*. Academic Press. doi:10.1007/978-0-12-001010-5

Lacity, M., Willcocks, L., & Feeny, D. (1995). IT Outsourcing: Maximize Flexibility and Control. *Harvard Business Review*, 73(3), 84–93.

Lee, G., & Xia, W. (2005). The Ability of information System Development Project Teams to Respond to Business and Technology Changes: A Study of Flexibility Measures. *European Journal of Information Systems*, 14(1), 75–92. doi:10.1057/palgrave.ejis.3000523

Lee, O., Banerjee, P., Lim, K., Kumar, K., Hillegersberg, V., & Wei, J. (2006). Agility in Globally Distributed System Development. *Communications of the ACM*, 49(10), 49–54. doi:10.1145/1164394.1164419

- Lin, C. T., Chiu, H., & Tseng, Y. H. (2005). Agility Evaluation Using Fuzzy Logic. *International Journal of Production Economics*, 101, 353-368. doi:10.1016/j.ijpe.2005.01.011
- Lin, C. T., Chiu, H., & Tseng, Y. H. (2006). Agility evaluation using fuzzy logic. *International Journal of Production Economics*, 101(2), 353-368. doi:10.1016/j.ijpe.2005.01.011
- Liu, S., Yang, Y., Qu, W. G., & Liu, Y. (2016). The business value of cloud computing: The partnering agility perspective. *Industrial Management & Data Systems*, 6, 116.
- Lu, Y., & Ramamurthy, K. (2013). Understanding the Link Between Information Technology Capability and Organizational Agility: An Empirical Examination. *Management Information Systems Quarterly*, 35(4), 931-954. doi:10.2307/41409967
- Lyytinen, K., & Rose, G. M. (2006). Information System Development Agility as Organizational Learning. *European Journal of Information Systems*, 15(2), 183-199. doi:10.1057/palgrave.ejis.3000604
- Markus, M., & Benjamin, R. (1996). Change Agency – The Next IS Frontier. *Management Information Systems Quarterly*, 20(4), 385-407. doi:10.2307/249561
- Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and Research. *Management Science*, 34(5), 583-598. doi:10.1287/mnsc.34.5.583
- McAvoy, J., Nagle, T., & Sammon, D. (2013). Using mindfulness to examine ISD agility. *Information Systems Journal*, 23(2), 155-172. doi:10.1111/j.1365-2575.2012.00405.x
- McCann, J., Selsky, J., & Lee, J. (2009). Building Agility, Resilience and Performance in Turbulent Environments. *People and Strategy*, 32(3), 44.
- Meade, L. M. (1997). Method for analyzing agility alternatives for business processes. In *Industrial Engineering Research - Conference Proceedings* (pp. 960-965). IIE.
- Mithas, Ramasubbu, & Sambamurthy. (2011). How information management capability influences firm performance. *Management Information Systems Quarterly*, 35(1), 237. doi:10.2307/23043496

- Overby, E., Bharadwaj, A., & Sambaurthy, V. (2006). Enterprise Agility and the Enabling Role of Information Technology. *European Journal of Information Systems*, 15(2), 120–131. doi:10.1057/palgrave.ejis.3000600
- Parger, K. (1996). Managing for Flexibility. *Information Systems Management*, 13(4), 41–44. doi:10.1080/10580539608907015
- Pereira, T., & Santos, H. (2010). A security audit framework to manage Information system security. In *International Conference on Global Security, Safety, and Sustainability* (pp. 9-18). Springer Berlin Heidelberg. doi:10.1007/978-3-642-15717-2_2
- Polónia, F., & de Sá-Soares, F. (2013). Key issues in information systems security management. *International Conference on Information Systems (ICIS 2013)*.
- Power, D. (2005). Supply chain management integration and implementation: A literature review. *Supply Chain Management*, 10(4), 252–263. doi:10.1108/13598540510612721
- Ramesh, B., Mohan, K., & Cao, L. (2012). Ambidexterity in agile distributed development: An empirical investigation. *Information Systems Research*, 23(2), 323–339. doi:10.1287/isre.1110.0351
- Richards, C. (1996). Agile manufacturing: beyond lean. *Production & Inventory Management*, 60-4.
- Rockart, J. F., Earl, M., & Ross, J. (1996). Eight Imperatives for the New IT Organization. *Sloan Management Review*, 38(1), 43–55.
- Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. *Management Information Systems Quarterly*, 27(2), 237–263. doi:10.2307/30036530
- Sarker, S., & Sarker, S. (2009). Exploring agility in distributed information systems development teams: An interpretive study in an offshoring context. *Information Systems Research*, 20(3), 440–461. doi:10.1287/isre.1090.0241
- Schapiro, S., & Henry, M. (2012). Engineering agile systems through architectural modularity. *Systems Conference (SysCon)*.

Schmidt, C., & Buxmann, P. (2011). Outcomes and success factors of enterprise IT architecture management: Empirical insight from the international financial services industry. *European Journal of Information Systems*, 20(2), 168–185. doi:10.1057/ejis.2010.68

Scott, J. (2007). Mobility, Business Process Management, Software Sourcing, and Maturity Model Trends: Proposition for the IS Organization of the Future. *Information Systems Management*, 24(2), 139–145. doi:10.1080/10580530701221031

Sharp, J., Irani, Z., & Desai, S. (1999). Working towards agile manufacturing in the UK industry. *International Journal of Production Economics*, 62(1-2), 155–169. doi:10.1016/S0925-5273(98)00228-X

Sia, S. K., Koh, C., & Tan, C. X. (2008). Strategic maneuvers for outsourcing flexibility: An empirical assessment. *Decision Sciences*, 39(3), 407–443. doi:10.1111/j.1540-5915.2008.00198.x

Soares, D., & Sá-Soares, F. d. (2014). Information systems security management key issues in local government. In *Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance (ICEGOV '14)* (pp. 227-230). New York: ACM. doi:10.1145/2691195.2691238

Sørensen, C., & Landau, J. S. (2015). Academic agility in digital innovation research: The case of mobile ICT. publications within information systems 2000–2014. *The Journal of Strategic Information Systems*, 24(3), 158–170. doi:10.1016/j.jsis.2015.07.001

Stettina, J. C., Kroon, & Egbert. (2013). Is there an agile handover? an empirical study of documentation and project handover practices across agile software teams. In *Engineering, Technology and Innovation (ICE) & IEEE International Technology Management Conference, 2013 International Conference on* (pp. 1-12). IEEE.

Susarla. (2012). Social Networks and the Diffusion of User-Generated Content: Evidence from YouTube. *Information Systems Research*, 23(1), 23–41.

Swafford, P. M., Ghosh, S., & Murthy, N. (2006). The antecedents of supply chain agility of a firm: Scale development and model testing. *Journal of Operations Management*, 24(2), 170–188. doi:10.1016/j.jom.2005.05.002

Tan, C., & Siew, K. (2006). Managing flexibility in Outsourcing. *Journal of the Association for Information Systems*, 7(4), 179–205. doi:10.17705/1jais.00086

Tanriverdi, H., Arun, R., & Venkatraman, N. (2010). Research Commentary: Reframing the Dominant Quests of IS Strategy Research for Complex Adaptive Business Systems. *Information Systems Research*, 21(4), 822–834. doi:10.1287/isre.1100.0317

Thompson, D. J. (1967). *Organisation in Action*. Academic Press.

Tiwana, A., & Konsynski, B. (2012). Complementarities between organizational IT architecture and governance structure. *Information Systems Research*, 288–304.

Truex, D., Baskerville, R., & Klein, H. (1999). Growing Systems in Emergent Organizations. *Communications of the ACM*, 42(8), 117–123. doi:10.1145/310930.310984

Vernadat, F. (1999). Research agenda for agile manufacturing. *International Journal of Agile*, 1(1), 37–40.

Volberda, H. (1996). Towards the flexible form: How to remain vital in hypercompetitive environments. *Organization Science*, 7(4), 359–387. doi:10.1287/orsc.7.4.359

Volberda, H., & Rutges, A. (1999). FARSYS: A Knowledge-based System for Managing Strategic Change. *Decision Support Systems*, 26(2), 99–123. doi:10.1016/S0167-9236(99)00023-8

Wang, X., Conboy, K., & Cawley, O. (2012). “Leagile” software development: An experience report analysis of the application of lean approaches in agile software development. *Journal of Systems and Software*, 85(6), 1287–1299. doi:10.1016/j.jss.2012.01.061

Wang, X., Conboy, K., & Pikkarainen, M. (2012). Assimilation of agile practices in use. *Information Systems Journal*, 22(6), 435–455. doi:10.1111/j.1365-2575.2011.00393.x

Weill, P., Subramani, M., & Broadbent, M. (2002). Building IT infrastructure for strategic agility. *MIT Sloan Management Review*, 44(1), 57–65.

Wenzler, I. (2005). Development of an asset management strategy for a network utility company: Lessons from a dynamic business simulation approach. *Simulation & Gaming*, 36(1), 75–90. doi:10.1177/1046878104272668

- White, A., Daniel, E. M., & Mohdzain, M. (2005). The role of emergent information technologies and systems in enabling supply chain agility. *International Journal of Information Management*, 25(5), 396–410. doi:10.1016/j.ijinfomgt.2005.06.009
- Woodard, C. J., Ramasubbu, N., Tschang, F. T., & Sambamurthy, V. (2013). Design Capital and Design Moves: The Logic of Digital Business Strategy. *Management Information Systems Quarterly*, 37(2), 537–564. doi:10.25300/MISQ/2013/37.2.10
- X, W., K, C., & M, P. (2006). Assimilation of agile practices in use. *Information Systems Journal*, 22(6), 435-455.
- Y, Z., W, V., & Cornford, T. (2011). Collective agility, paradox and organizational improvisation: the development of a particle physics grid. *Information Systems Journal*, 21(4), 303-333.
- Yi, C. Y., Ngai, E. W., & Moon, K. L. (2011). Supply chain flexibility in an uncertain environment: Exploratory findings from five case studies. *Supply Chain Management*, 16(4), 271–283. doi:10.1108/13598541111139080
- Yin, R. (2013). *Case Study Research, Design and Methods* (5th ed.). Sage Publications.
- Yusuf, Y., Sarhadi, M., & Gunasekaran, A. (1999). Agile manufacturing: The drivers, concepts and attributes. *International Journal of Production Economics*, 62(1-2), 33–43. doi:10.1016/S0925-5273(98)00219-9
- Zhang, Z., & Sharifi, H. (1999). A methodology for achieving agility in manufacturing organizations: An introduction. *International Journal of Production Economics*, 62(1-2), 7–22. doi:10.1016/S0925-5273(98)00217-5
- Zheng, Y., Venters, W., & Cornford, T. (2011). Collective agility, paradox and organizational improvisation: The development of a particle physics grid. *Information Systems Journal*, 21(4), 303–333. doi:10.1111/j.1365-2575.2010.00360.x

Chapter 5

IT Management Agility in Large Organizations: A Case Study

ABSTRACT

A successful IT service and asset management need to be efficient and agile to help transform from a traditional into a digital enterprise. In this chapter, the authors propose a global and practical strategic framework to improve ITSM service management processes with the additions of two drivers: agility management based on DevOps and security management based on SecOps. The proposed framework will affect all aspects of user productivity DSI oriented and implement an agile approach in the heart of the management of all these aspects. They will study a case of application of the proposed framework on a large company and the gain made on the strategic level and decision making. The authors propose to measure the maturity of the ITSM of the organization and set up their benchmark to improve IT governance through the proposed ITSM framework.

DOI: 10.4018/978-1-5225-7826-0.ch005

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Context

Agile mode projects are increasingly popular among the IT department, including the most complex organizations. The deployment of agility on a larger scale fits over a long period because the motivations are part of a persistent setting. The deployment of large-scale agility is therefore based on a deep and lasting transformation of the organization.

Faced with the global systemic crisis that acts as an accelerator of change, companies must find ways to adapt continuously. For CIOs, the promises of agile methods fully meet these expectations. A transformation strategy to Agile for CIOs is the creation of an Agile Services Center. Agility is all about innovating and the ability to react quickly, efficiently and effectively to external factors. For IT, it is the capacity to deliver new IT services in support of new business processes that are at the core of IT agility.

Purpose

In order to support transformational business change, IT needs to streamline the process of bringing new IT processes to life.

In today's ever-changing business world, nobody knows what's around the corner, so improving agility is the best way to future-proof organization.

By defining what IT maturity looks like in your organization, you can plot a route to successive levels of maturity and improved agility to reach a point where IT help run, grow and quickly transform the business.

IT Service Management is the ability to collect data, analyze it, to make reports and to implement improvements in agile mode, sometimes make it difficult to effectively manage all these informational organization assets. To perform a real-time monitoring of these activities, manage, and be able to involve the final user in the heart of the IT process, or reduce operating cost, agility is the ideal solution.

In this work, we propose a global strategic model to improve ITSM service management processes with the additions of two drivers Agility management and security management. The proposed framework will affect all aspects of user productivity DSI oriented and implement an agile approach in the heart of the management of all these aspects.

Approach

According to Brooks (2006) IT service management tools deals with many IT service management measurements and most of it will be interesting to people in the related departments with the same activities. Metrics are identified to show development and the performance of the system. Therefore, there are three types of metrics to improve the quality level of the evaluation framework such as, effectiveness, capabilities and efficiency. These elements could be matched into any technology, process or service that focuses on Operational Level (Service Support Domain), Tactical Level (Service Delivery Domain) and Strategic Level.

The chapter aims to identify the important aspects that propose a comprehensive framework for ITSM efficiency. It was collected of a theoretical and empirical research study that generated answers to the sub-level research questions. The author tried to extract a framework based on the literature review and various sources from the practical environment. The framework was used within the far-reaching empirical study to find ways to compare and identify different corporation metrics. The organizations becoming more reliant on a comprehensive framework to control IT service management in organizations; how ITIL-ITSM best practices have an effect on organization efficiency and problem-solving.

The IT department's responsibility for maintaining and securing the IT environment now includes all devices employees use, but budgets and IT resources are limited. The framework ITSM proposed exploits the good practices ITIL and ISO 2000 and integrates new strategic axes such as agility and security in order to propose an efficient and agile IT service management. It replaces the traditional IT services of the "control and control" type, oriented peripherally by a complete integrated, user-oriented approach with the integration of four disciplines of IT management (Service management, Security management, Agility management and Asset management).

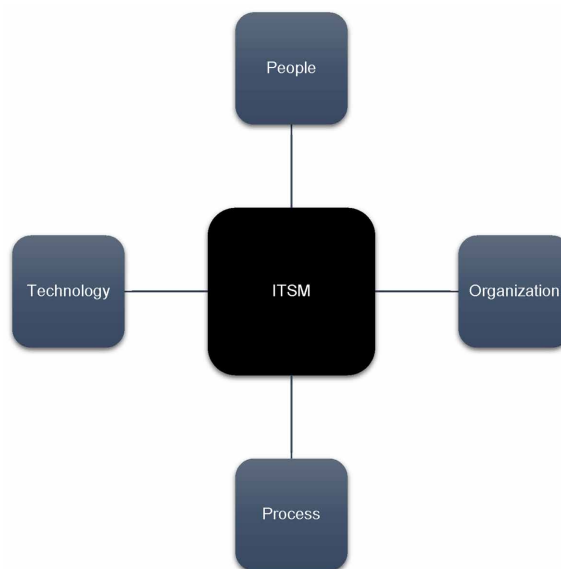
The IT department's responsibility for maintaining and securing the IT environment now includes all devices employees use, but budgets and IT resources are limited. Agility is the right solution for IT departments to streamline IT processes and manage all aspects of end-user productivity. The objective is to reinforce the traditional IT services of the "control and control" type, oriented peripheral by a complete integrated approach, oriented user. ITSM increases the level of the communication efficiency between business departments and provides a structure to plan, research and implement

IT Management Agility in Large Organizations

IT services. The needs of IT service management in organizations can be changes in the ways they do business, communicate and also develop and innovate, gain market advantage and differentiate themselves to their customers (Brooks, 2006). Also, ITSM allows companies to internally govern and follow to the set global standards (Mior, 2008). For a better understanding of the ITSM concept in the organization, reviewing the ITSM component would be useful. ITSM components consist of Process, Technology, Manpower (people), Organization, and Security, which is recently added to organization construction to improve the system security (Park, 2008; McNaughton, 2010). Figure 1 illustrates the component of ITSM.

- **Processes:** The most important element to construct the ITSM (e.g.IT business process facilitates and keeps up IT service).
- **Organization:** To provide better IT service level and arranges proper tasks in the organization.
- **Technology and Security:** To provide the best possible tools and automated solutions to develop a process with a higher level of efficiency and safety.

Figure 1. ITSM components



As mentioned earlier, IT service is connected to the four fundamentals of Information Technology Service Management (ITSM). Therefore, when IT is aligned with the business strategy and the organization, it can do what it wants to do. Furthermore, IT and new technologies enable the organization to do new things that were never possible before (Silva Molina, 2005). The strategic outcome is that the overall business benefits from effective IT-related service and IT benefits that are integral to the company's business plans will be delivered to the maximum economic value.

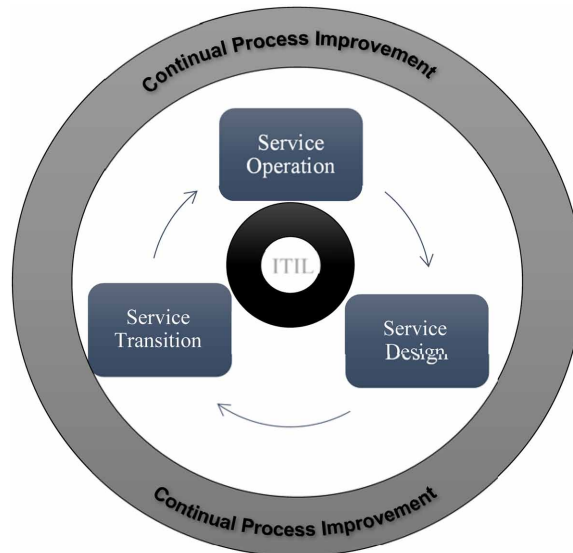
In the literature and even references such as ITIL, ISO 20000, Cobit (van Grembergen, 2009), there is no practical, concrete and agile model for the implementation of IT services and assets management in organizations. In this work, we propose a global, practical and agile framework for supporting IT Service management ITSM and IT Asset Management ITAM. The proposed framework surpasses the limitations of existing methods/referential and meets the needs of international standards regarding flexibility and agility to improve ITSM/ITAM processes. This generic framework will help any organization in the implementation of an agile, secure and optimal IT Service Center. We measure the proposed framework by adopting a continuous improvement process based on DevOps (DevOps is the concatenation of the first three letters of the word "development" and the usual abbreviation "ops" of the word "operations") and the PDCA Deming cycle.

RELATED RESEARCH

ITSM in Referential ITIL, ISO 20000

ISO 20000-1 is based on ITIL, which presents a set of best practices for the management of information systems. This approach and vision to IT service management highlight the importance of coordination and control of various functions, processes, and systems required to manage the full lifecycle of IT services. The following Figure 2 presents in a simplified way an overall representation of the process vision according to ITIL. The latter is broken down into a cycle consisting of five phases: service strategy, service design, service transition, the operation of services and continuous improvement of services. Also, document management, resource management, and service governance align with all phases of the service lifecycle, processes.

Figure 2. ITIL Process



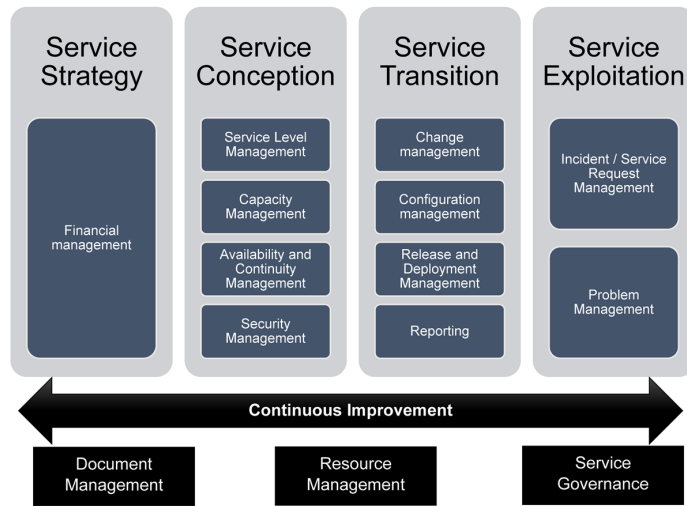
More explicitly, the following Figure 3 presents the existing processes in each phase of the service lifecycle in the context of ISO 20000.

ITSM/ITAM in Scientific Research

During the last two decades, the ITSM-related frameworks have provided a better systematic approach to the management of IT services in the fields of IT operation to continual improvement, implementation, and design (Marrone, 2011). For example, different studies have concentrated on the adoption of IT Service Management (ITSM) as a “particular service-oriented best practice”. According to Winniford (2009), about 45% of US corporations are operating an ITSM while 15% are preparation its usage. IT service management is somehow the quality customer service that tries to ensure that customer needs and expectations are met at all times (Tan, 2009).

In “ITIL: What It Is And What It Isn’t,” Hank (2006) examined in the measuring techniques of successful companies when implementing the ITIL-best practice. He describes Service Support and Service delivery and explains its stress on an ITSM-ITIL best practice that it does not stand alone, and it could be successful when applying to other practices. The authors define three major tasks, which define appropriate goal setting through a Process Maturity Framework (PMF), rigorous auditing and reporting through a Quality

Figure 3. The Process Model of ITSM_ISO 20000



Management System (QMS) and Project Management and a Continuous Service Improvement Program (CSIP), to support ITIL-usage. Furthermore, he also provided more information about business-aligned IT process and continuous improvement of the tactical and operational components especially those processes that focused on service quality by clients and users (Hank, 2006).

Apart from the other works on improving the efficiency of IT service management field, there is a real-life example of a case study, which is focusing on IT framework, and Service Strategy process of Steel Manufacturing Enterprise (SMC). In a manufacturing enterprise, Zhong (2010) used integration of COBIT and ITIL best practice to implement and improve ITSM framework. They introduced an approach to service strategy evaluation framework in SMC by providing indicators for the different evaluation process to improve the result from ITIL implementation and to increase the improvements on changed IT processes; they use different approaches to find the problem of Business-IT-alignment in SMC. The approach aims at minimizing the difficulty of business-IT-alignment in importance within the IT community. In the same article, Bartolini (2006), has suggested an IT Management by Business Objectives (MBO) method, which is a unique way to ensure business strategic objectives-IT alignment, by defining a new system for decision support in ITSM. It is closely related to the ITIL component in operational level and tactical level of theoretical.

In “E-government: ITIL oriented Service Management Case Study”, Meziani (2010) developed a service management self-assessment plans for the government agency to support the continuous quality improvement of IT processes based on ITIL governance- gap analysis methods with respect to ITIL standards (Meziani and Saleh).

In Their work entitled “Managed IT-Services: the role of IT standards”, Kumbakara (2008) argues the practical issues based on standards and the management of IT services delivered by external or outsourced service providers. Here, the purpose of the authors is to assist IT organizations to recognize the significance of having a mutual standard for managing IT services.

van Grembergen (2009) illustrated a set of best guides and practices (COBIT Framework) for IT management control and assurance of information technology and categorized them around a logical framework based on 34 IT processes.

Marrone (2011) studied the benefits of both operational and strategic of IT Service Management. The research outcome indicates that as the implementation of ITIL increased the number of realized benefits, like the levels of maturity of the Business-IT-Alignment.

In his book entitled “Information management: the evaluation of information systems investments” (Wilcocks, 2013). The author proposes different approaches to evaluating practice at strategic levels and during the pre-purchase phase of IS assessment. In the book “Asset management: A systematic approach to factor investing”. The authors (Ang, 2014) introduces a comprehensive and new approach to the secular problem of where to place your money in the IT Asset Management. In recent works “Reducing the cost of test through strategic asset management” (Duane & Charlie, 2016). The authors explore the balance of the three fundamental aspects that make up asset management and will focus on how to implement strategies to reduce the total cost of ownership for the test.

Agility in Literature

The concept of agility was first used in the literature of strategic management and industry at the beginning of the years (Meade, 1997; Vernadat, 1999; Yusuf, Sarhadi, & Gunasekaran, 1999; Richards, 1996; Goldman, 1995). Agility was introduced and proposed in the literature, with the argument that success in volatile industries requires a set of capabilities different from success in stable

industries (Volberda, 1996; Volberda & Rutges, 1999) In such situations, the organization must be agile and able to capitalize and respond to opportunities generated by new market situations faster than their competitors (Goldman, 1995). The key question then is: how can an organization become agile? How can they create the required capabilities? Moreover, perhaps more broadly, what are exactly these capabilities? This subject was addressed in several areas of strategic management and organizational studies, rooting the theory that began well before the introduction of agility concept.

In IS research, the agility concept has been Introduced in early 1990 (Ciborra, 1992; Markus & Benjamin, 1996; Clark, Cavanaugh, Brown, & V, 1997; Sharp, Irani, & Desai, 1999; Zhang & Sharifi, 1999)). After the success of agile methods in computer development. In research, the concepts of flexibility and agility have been associated with the broader challenge of combining complex computer systems with unexpected changes, sometimes surprising in user needs, business processes, company structure, strategy, markets, and society in overall. At the beginning of the year 2000, the emphasis was on other attributes of (IS) explain agility through IT, development methods (IS) and IS outsourcing practices.

Guided by our research question, we have used a provisory classification as shown in Table 1, to identify research that addresses the relationship between ITSM/ITAM and agility. In the literature, we deduced that is a lack of a unique definition of the agility concept. The Agility Research in (IS Agility) was devised on several axes (Lee, et al., 2006; Fink & Neuman, 2009; Holmqvist & Pessi, 2006; Hong, Thong, Chasalow, & Dhillon, 2011). Table 1 highlights the main IS/IT agility research streams.

Table 1. Information system agility research streams

IS agility research streams	Authors
IS Design and Governance	(Rockart, J.F., Earl, & Ross, 1996) (Parger, 1996) (Clark, Cavanaugh, Brown, & V, 1997) (Boar, 1998) (Truex, Baskerville, & Klein, 1999) (Tan & Siew, 2006) (Gerth & Rothman, 2007) (Sia, Koh, & Tan, 2008) (Stettina, Johann, Kroon, & Egbert, 2013)
Strategic IS management	(Lacity, Willcocks, & Feeny, 1995) (Sia, Koh, & Tan, 2008) (Schmidt & Buxmann, 2011) (Tiwana & Konsynski, 2012) (Joachim, Beimborn, & Weitzel, 2013)

IT Management Agility in Large Organizations

IS agility research streams	Authors
Competencies and Skills of IS professionals	(Markus & Benjamin, 1996) (Butler & Gray, 2006) (McCann, Selsky, & Lee., 2009)
IS Development	(Baskerville & Pries-Heje, 2004) (Lee & Xia, 2005) (Holmqvist & Pessi, 2006) (Lyytinen & Rose, 2006) (Conboy, 2009) (Sarker & Sarker, 2009) (Zheng, Venters, & Cornford, 2011) (Hong, Thong, Chasalow, & Dhillon, 2011) (Ramesh, Mohan, & Cao, 2012) (Wang, Conboy, & Pikkarainen, 2012) (McAvoy, Nagle, & Sammon, 2013)
Methods of Software development	(Overby, Bharadwaj, & Sambaurthy, 2006) (Börjesson, Martinsson, & Timmerås, 2006) (Scott, 2007) (Dybå & Dingsøy, 2008) (Tanriverdi, Arun, & Venkatraman, 2010) (Stettina, Johann, Kroon, & Egbert, 2013)
Design of IT infrastructure	(Allen & Boynton, 1991) (Duncan, 1995) (Byrd & Turner, 2000) (Benamati & Lederer, 2001) (Wenzler, 2005) (Overby, Bharadwaj, & Sambaurthy, 2006) (Dybå & Dingsøy, 2008) (Park & Kim, 2008) (Fink & Neuman, 2009) (Tan C.-S., 2009) (Tanriverdi, Arun, & Venkatraman, 2010) (Schmidt & Buxmann, 2011) (Schapiro & Henry, 2012) (Celen & Djurdjanovic, 2012) (Joachim, Beimborn, & Weitzel, 2013) (Yin, 2014)
Business agility and the value of IS applications	(Broadbent, Weill, & St.Clair, 1999) (Rockart, J.F., Earl, & Ross, 1996) (Lee & Xia, 2005) (Scott J., 2007) (Gerth & Rothman, 2007) (Gerth & Rothman, 2007) (Gebauer & Schober, 2008) (Gebauer & Schober, 2008) (Fink & Neuman, 2009) (Tanriverdi, Arun, & Venkatraman, 2010) (Bhatt, Emdad, Roberts, & Grover, 2010)
Agility in IT Service Management	(Izza, S., & Imache, 2010) (Abdelkebir, Maleh, & Belaiassaoui, 2017)

However, there is a lack of research regarding agility in IT Management Systems. Although the IT function, in all its dimensions, gains in flexibility, and in reactivity. Beyond that, the IT system function is at stake and must have the capability to accelerate its adaptation to business needs, market requirements, and the strategic alignment of the IS and the organization. Agility is the best solution to cope with the different internal/external changes ... DevOps is a set of best practices and changes guidance that ensures development, assurance and quality improvement and operations to respond effectively better to customer needs. Patrick Debois invented the word DevOps during the organization of the first DevOps days in Ghent, Belgium, in October 2009. To ensure competitiveness, the organization must accelerate the delivery of new functionalities and software features. This is the idea behind agile application/software development processes that are now widely used by application delivery teams to reduce delivery cycle times. DevOps can be applied in the ITSM/ITAM field, in order to benefit from it and to ensure an efficient and flexible ITSM/ITAM in the organization. In recent work (Gene, Jez, Patrick, & John, *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations*, 2016). The authors argue that more than ever, effective technology management is essential for business competitiveness. For decades, technology leaders have struggled to balance agility, reliability, and security. The book does not focus on tools such as infrastructure such as code, containers or configuration management. These are people, culture, and processes. The book creates a language to describe DevOps and a common understanding. Highly recommended, no matter if you have a professional or technical environment. The DevOps Handbook shows leaders/practitioner how to reproduce these incredible results, showing how to integrate IT operations, development, product management, quality assurance, and information security to raise your business and win in the market. DevOps helps the organization to bring together key players (companies, applications, and ops) with a focus on collaboration, automation, and monitoring, resulting in better application delivery speed with quality. Here are some of the ways DevOps helps to generate business value.

- **Obtain a Competitive Advantage:** Accelerate the output of applications in production. Faster response to business demand.
- **Increase the Efficiency of IT Resources:** Automate provisioning and deployment. Delete the manual processes.

- **Enable Better and Faster Decisions:** Create an immediate feedback loop. Identify problems earlier in the process.
- **Hang on to Business Requirements:** Bring new applications and updates to the market quickly to create satisfied customers.

In recent work, Abdelkebir et al. (2017) proposed a holistic and practical strategic framework to improve ITSM service management processes with the additions of two drivers Agility management based on DevOps, and an agility Process Maturity Framework (APMF).

In this chapter, we propose an extended and detailed version of the proposed framework.

THE PROPOSED ITSM/ITAM FRAMEWORK

ITSM/ITAM increases the level of the communication efficiency between business departments and provides a structure to plan, research and implement IT services. The needs of ITSM/ITAM in organizations can be changes in the ways they operate, communicate and do business and also develop and innovate, gain market advantage and differentiate themselves to their end customers (Brooks, 2006). Also, ITSM/ITAM allows companies to internally govern and follow to the set global standards (Mior, 2008).

However, the types of the ITSM/ITAM benefits and allocation among stakeholder group can be different based on the purpose of the system and managerial goals. Therefore, to attain the maximum level of efficiency, we must first identify IT and business goals to understand better the needs of organization, managers, and stakeholders. According to (Jurison, 1996), “stakeholders are all those parties who affect or are affected by a corporation’s actions, behavior, and policies. Thus, IT investment made by the stakeholder or IT management based on different business demands can be issues mentioned below:

- Take customers as a center and provide IT service that meets customer’s needs.
- Enhanced quality.
- Low cost IT service in the company.
- Better response to the client needs.
- Evaluating service delivery.

In the last part, we have proposed different feedbacks about the ITSM/ITAM concept in the organization. In this section, it would be helpful to be able to provide our practical framework, which has been missing in the Service Quality of IT Service Management process with some suggestion to improve different approaches, which we have evaluated.

It seems that there are many problems in having a successful ITSM/ITAM process. Conversely, as identified before, many good efforts have been made to improve these issues. For a better understanding of the concept of these challenges, there are three possible approaches to improving ITSM/ITAM efficiency, which are:

Many academic and industrial efforts have been made in many IT corporations to improve the Quality Measurements of business-IT alignment. Researchers like, Das (1991), Reich, (2000), and Luftman (2003) used multi-dimensional scales to measure the business IT-alignment. The result from our interviews and collected metrics exposed some important elements to improve the efficiency of ITSM. The IT service management meets the need to align the IT services delivery directly with the requirements of the business. Some of these concerns and issues are reflected in this organization to provide ITIL-best practices and to deliver a comprehensive and useful IT service management framework.

ITIL-ITSM best practice is not a one-time process; it is an ongoing activity to control system performance. According to Porter (1996) continuous improvement is needed to remain relevant in the market. Through our case study, we came to know that the target groups of our research chapter are almost employing the same methods, but there is a small difference in IT service management process and measurement implementation. According to Brooks (2006) IT service management tools deals with many IT service management measures and most of it will be interesting to people in the related departments with the same activities. Metrics are identified to show development and the performance of the system. Therefore, there are three types of metrics to improve the quality level of the evaluation frameworks like effectiveness, capabilities, and efficiency. These elements could be matched with any technology, process or service that focuses on Operational Level (Service Support Domain), Tactical Level (Service Delivery Domain) and Strategic Level.

The chapter aims to identify the important aspects that propose a comprehensive framework for ITSM/ITAM efficiency. It was collected in a theoretical and empirical research study that generated answers to the sub-level research questions. We tried to extract a framework based on the literature

review and various sources from the practical environment. The framework was used within the far-reaching empirical study to find ways to compare and identify different corporation metrics. The organizations becoming more reliant on a comprehensive framework to control IT service management in organizations; how ITIL-ITSM best practices affect organization efficiency and problem-solving.

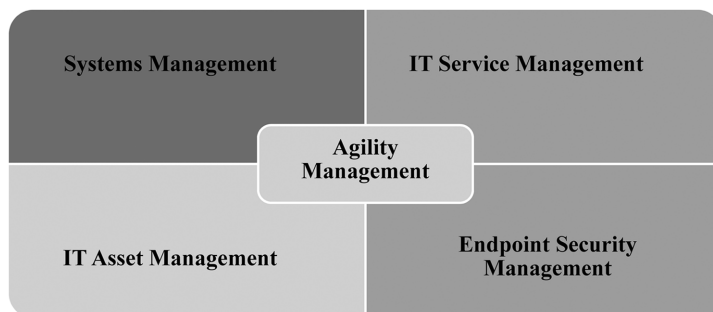
The IT department’s responsibility for maintaining and securing the IT environment now includes all devices employees use, but budgets and IT resources are limited. The framework ITSM/ITAM proposed exploits the good practices ITIL and ISO 2000 and integrates new strategic axes such as agility and security to offer an efficient and an agile ITSM/ITAM. It replaces the traditional IT services of the “control and control” type, oriented peripherally by a complete integrated, user-oriented approach with the integration of four disciplines of IT management (Service management, Security management, Agility management and Asset management). Figure 4 describes the architecture and the component of the proposed ITSM/ITAM framework.

IT Service Management ITSM

Most of the ITSM Organizations consider Service Support process as a difficult task. Difficulties are mainly due to the following reasons:

- IT organizations do not have a structured approach for measuring IT service and service management processes.
- Different tools exploited by IT Support Service Teams do not enable effective measurement.

Figure 4. The proposed ITSM/ITAM model



- IT service management standards and frameworks do not provide practical examples on how to measure support process (Lahtela, 2010).
- Therefore, IT organization needs a structured approach for measuring IT service support process such as ITIL V2/V3 or the other reliable sources to increase IT quality of services. So, implementations of the service support process are chosen as a priority to help as a result of continuous improvement in ITSM.

As it's illustrated in Table 2, IT service support process includes five main steps (Wui-Gee, 2009).

Incident Management

An incident is an intimation of some errors or the failure of some components in an IT system. In a typical service desk center, the incident is reported by the client or automatically generated by the monitoring system (Gupta, 2008). The primary goal of an incident manager is to minimize interruption in the business activities and ensure availability of service.

Table 2. IT service support process

Service Support Process	Description	Example
Incident Management	Restores normal service operations as quickly as possible	"Virus Attack, Server crashes. Hardware alarm, Turn down and decline of system performance" (McNaughton, 2010)
Problem Management	Prevents incidents from happening and minimizes the impact of incidents that cannot be prevented	"All incidents that are not fixed basically with known errors" (McNaughton, 2010)
Change Management	Controls the lifecycle of all changes	
Release Management	Implements approved changes to IT services	"To provide a solution for the problems like parameter, adjust, patch, configuration changes, upgrade to system version and server".
Configuration Management	Maintains information on Configuration Items required to deliver an IT service, including their relationships	"Tracking, Reporting and controlling all equipment's". (McNaughton, 2010)

Service Desk

Service desks are requested to report IT problems in the enterprise system. It is a single point of contact (SPOC) which is basically for the users who need assistance for operating their IT systems, such as incident management, configuration changes, information and customer's problem which is managed by a level-1 person. Moreover, the Service desk owns and manages various tasks, such as dealing with tracking and communication by handling the closure phase and transmitting messages. The Service Desk is known as the "Notification" which is in different cases function (Gupta, 2008). For example, Incident is an indication of some errors in an IT system component; the majority of historical database incidents are maintained at the service desk.

Configuration Management

Is responsible for managing the information about configuration items required to deliver a service (Meziani, 2010). There are some indicators for the configuration management such as "rate of change management failures caused by original information errors, the rate of no corresponding request service items, the rate of unable to execute configuration after changes occurred" (Meziani, 2010).

Change Management

This is an efficient process for implementing changes required by the organization. All the changes must be evaluated, approved, implemented, and checked. Some of the indicators of change management are the rate of change failure, the rate of necessary change, the rate of unable to execute the change management process, service interrupt caused by the change.

Release Management

It is a way to communicate and manage expectations of the customer during the planning and rollout of new releases. For example, for each server, "there should be built an account for all equipment with attributes such as the type, configuration, duration of equipment, diagnosis history, change and repairing reports" etc.

Service Level Management (SLM)

The goal of Service Level Management (SLM) is to maintain and improve IT service quality, monitoring and reporting upon IT service achievements and investigation of actions to eliminate poor service.

Problem Management

A problem is the unknown cause of a significant incident or several incidents with the same symptoms affecting the proper functioning of the company's information system or "business". The objective of problem management is to minimize the impact of incidents and challenges on the firm and to prevent their occurrence by anticipating through predictive/proactive corrective actions. It is about solving the dysfunctions by organizing and controlling the use of resources.

Self-Servicing

In the area of IT service management, there are considerable advantages in enabling users to solve problems themselves. He answers this old saying about the difference between giving fish and teaching people how to catch all the fish by themselves. For the average user - either customers or employees using a website, application or SaaS (Software as a Service), self-service offers those capabilities that in the past were exclusively in the domain of IT technicians and Service Desk. The service center must resolve problems quickly and more efficiently, but we face it; Achieving high performance in IT service support is often easier said than done. Long delays, the commissioning of an operator, false communication, etc. All contribute to longer resolution times. Sometimes the best way to solve customer problems is to give them the tools to find solutions for themselves. Self-service ignores the trouble of bringing people into the mix and allows end-users to quickly find what they need and run on a single solution.

Configuration Management Database CMDB

The CMDB as defined is the federated and integrated base allowing feed many processes: Incident Management, Problems, Release, Change, Capacity, Availability, Continuity, Financial, Asset Management & Configurations.

IT Management Agility in Large Organizations

- Identification of CIs and associated attributes,
- Lifecycle management of configuration elements, from the point of entry to flow,
- A complete history of all activities related to a configuration item (displacement, technical evolution, ...),
- Intuitive modeling of relations between CI,
- Impact analysis on IS, on users
- Valuation of assets,
- Contract management.

ITSM Maturity Model

The scope of the evaluation would cover only the key processes of the service operation and the service transition. Data are collected through interviews, workshops, literature review and site visits. Visits to the service desk and data center may be required. A list of questions is often used. A time-based assessment would aim to determine the level of maturity of each ITIL process. Other data to be collected include the availability of tools, competencies, the role, and responsibilities of the organization, availability and quality of documentation, evidence of continuous improvement, measurement and reporting, dissemination and the use of reports. By the answers to the questions collected, the scores are tabulated using a spreadsheet tool and presented. A time-based assessment can use the 5-level ITSM maturity model to evaluate the individual process of ITSM as shown in Table 3.

IT Asset Management (ITAM)

Today, in the challenging economic environment, knowing what assets you own, how they are used and where they are physically and in a business context is essential.

Without this information, it is tough to plan, plan and budget the company's IT resource requirements. Furthermore, without information on the nature of the possessions and their use, it is impossible to guarantee compliance with regulatory and contractual obligations.

Knowing and mastering this valuable information can help to solve many of the pressing problems that arise today, including:

Table 3. ITSM maturity model

Maturity Level	Description
Level 1: Initial	Awareness of the existence of the problem and the need to study it. However, there are no standardized processes, but approaches in this direction tend to be applied individually or on a case-by-case basis. The global management strategy is not organized.
Level 2: Reproducible	The organization makes significant efforts to develop and establish the management process for ITSM services. The notions of reactivity and short-term are there. At this level, the organization is a little more advanced in its management. The activities related to this process are not all coordinated and are irregular. Commitment to the process is evident in the allocation of resources. However, IT service management is not always formalized or compliant.
Level 3: Defined	Describes a formalized service management process in which the objective, activities, inputs, and outputs have been defined. The performance is consistent and can be repeated throughout the organization. The process is developed, implemented and managed in a satisfactory manner in its entirety. The management process is identified and documented but there is no recognition of its role within the IT organizations as a whole. However, the process has a manager, formal objectives, and dedicated resources. A reporting is put in place to capitalize on the experience.
Level 4: Managed	It is possible to monitor and measure ITSM compliance to standards and to act when processes do not seem to work properly. The management of the services is continuously improving and corresponds to good practice. Automation and the use of tools are limited or partial.
Level 5: Optimized	IT service management has reached the level of best practice, following constant improvement and comparison with other similar contexts. The technology is used as an integrated way to automate workflows, providing tools that improve quality and efficiency and make the company quickly adaptable.

- Provide decision-makers with detailed information on the allocation, cost, and forecast of assets
- Reduce risk by avoiding penalties and expensive litigation due to regulatory or contractual non-compliance, especially in software licensing
- Implement asset responsibility with management reporting to optimize the use of assets and protect against malicious use and theft
- Reduce costs by eliminating unnecessary acquisitions if the property already exists
- Proactively manage the warranty and support and maintenance contracts for optimal utility
- Negotiate better contracts by properly managing assets and suppliers
- Improve productivity by automating the flow of goods in your environment
- Facilitate data-based internal compliance and accountability audits to improve processes continuously

Asset management enables the collection of hardware, software and system data from managed machines in the IT infrastructure. In this way:

- Provide decision-makers with detailed information on the allocation, cost, and forecast of physical and software assets
- Proactively manage the warranty and support and maintenance contracts for optimal utility
- Facilitate data-based internal compliance and accountability audits to improve processes continuously

The information collected may include data on:

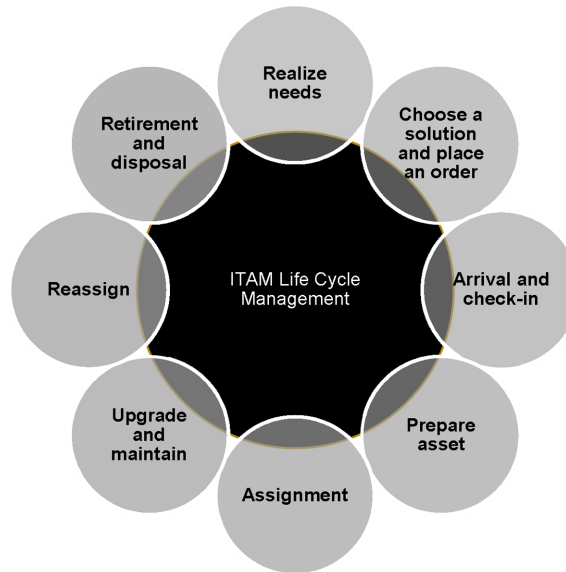
- Hardware: disk, memory, processor, network card, sound card, graphics card ...
- System: BIOS, ports, system configuration ...
- System environment: OS, patch, environment variable, processes, domain, users, network shares ...
- Devices: keyboard, mouse, display, storage device, printer ...
- Software

ITAM Lifecycle Management

Most people understand the value of managing software assets correctly. However, what about asset management? Can you find cost savings by monitoring hardware assets such as desktops, laptops, printers and other consumables within the organization? Asset management delivers real results, extending the scope of asset management (ITAM) while saving significant amounts of money and resources. Hardware/software asset management are closely linked. You cannot have one without the other. When a new software request is received, the hardware on which it is to run must be aware that many software applications require specific hardware to function properly or efficiently. We define an eight-step ITAM model of material lifecycle management, as illustrated in Figure 5, to ensure no item goes unaccounted.

- **Realize Needs:** Tracking demands to meet user needs and to foster future growth.
- **Choose a Solution and Place an Order:** Use workflow features to make informed decisions from repository data.

Figure 5. ITAM lifecycle management



- **Arrival and Check-In:** Takes advantage of primary assets for change management and relationship monitoring.
- **Prepare Asset:** Install appropriate software on assigned devices for accurate license monitoring.
- **Assignment:** strategically allocate and distribute resources.
- **Upgrade and Maintain:** Connect support resources such as information, contracts, and warranty and rental data.
- **Reassign:** Clean the device for reassignment and follow-up.
- **Retirement and Disposal:** Erase data, recover software and dispose of physical assets.

ITAM Achievement Model

The ITAM maturity model is a proposed roadmap to help ITAM managers define a direction for their programs. For an organization that already has ITAM in place but may be stuck in the phase of responding to software audits and not evolving beyond that, the proposed maturity model could be used as a roadmap for defining the next steps and expand the use of assets organizational data to help solve problems in other computer domains. Organizations often find it difficult to articulate the business case for the implementation of asset

management. This implementation model helps in this effort by identifying the problems to be solved and their priority to evolve successfully to the next level of achievement. Progression from one level to another requires knowing what should be accomplished first to succeed in the next step. Sometimes an organization may ignore a step, but the overall result will be more efficient if the progression occurs. In conjunction with process frameworks, questions on how to follow these steps can be answered. Keep in mind that the movement through the implementation model requires resources and dedicated efforts to get the benefits. One of the challenges encountered in proposing this model was the role of an organization that identified the next steps of the ITAM program. These programs can be aligned with IT operations, and they are frequently aligned with IT procurement, procurement, vendor and contract management. This creates an enigma, as it would be difficult to identify the steps for each role that might be interested in ITAM. Therefore, we have tried to do it at a high level. Also, this model will not be applicable to businesses of all sizes. Small businesses may not have the staff or funds to invest in the advancement of their ITAM program. The achievement model begins by looking at the components of an effective ITAM discipline: governance, policies, processes, people, metrics, automation, and alignment with business direction. Table 4 describes the ITAM achievement model.

Table 4. ITAM maturity model

Level 0: Unmanaged	Level 1: Initial	Level 2: Managed	Level 3: Optimised
<ul style="list-style-type: none"> ▪ No Leadership ▪ No Tools ▪ No Process ▪ No Standards ▪ No Visibility ▪ Audit-driven ▪ Decentralized 	<ul style="list-style-type: none"> ▪ Service Desk Leads ▪ Helpdesk Tools ▪ Incident, Request Processes Only ▪ Manual ITAM ▪ No Policy ▪ No Standardization ▪ No Knowledge 	<ul style="list-style-type: none"> ▪ IT Ops Leads ▪ Change & Release Tracked ▪ Configuration / Basic CMDB ▪ Basic Problem ▪ Knowledge DB 	<ul style="list-style-type: none"> ▪ Business/ Board Leads ▪ Business Portfolio Mapped to Systems ▪ Supplier Performance ▪ Financial ▪ Innovation ▪ Risk

- **Level 0: Unmanaged:** As far as asset management is concerned, it is non-existent at entry level. We do not spend much time characterizing this level because ITAM does not happen systematically. There are many reasons why an organization has not implemented ITAM. For example, the company may be too small, highly distributed, does not recognize ITAM as a priority when there are other issues with increased visibility, does not have enough staff, or is not in growth mode. It is difficult for organizations and firms to develop a roadmap at this stage, as they do not have sufficient resources/staff/funds. Other attributes of an ITAM program, such as governance, staffing, processes, policy, and parameters, are not considered at this level. As a result, costs and risks are high, delays are extended and the quality of service is low.
- **Level 1: Initial:** This initial level is the place where we attend the majority of the organization and the companies that undertake an ITAM program. They recognized the problems that need to be addressed systematically. This knowledge can come from a verification of software vendors, a lost mobile device that contains sensitive data or for several reasons. At this level, costs and risks are high, delays are extensive, and the quality of service is deficient. Essentially, it 's hard for end users to do their job effectively when they do not have the resources to support them. Since there is a well-documented skill shortage for skilled ITAM professionals, most companies succeed by training internal staff to fill open roles. There are no magic numbers to organize a program, but it tends to be higher in the early stages of program implementation so that stakeholder support is essential if the workforce needs to be shared.
- **Level 2: Managed:** The managed level is what each ITAM program should strive to achieve so that the company has confidence in the ability of computing to fulfill its charter. While all characteristics are not documented and deeply rooted in information technology, the business unit finds that the risks, costs, and delays are too high or extended, while the quality of service is low. When frustration arises, ITAM programs are outsourcing targets after costly audits or security breaches. At this level, policies must be in place. However, policies are targeted at the behavior of end users, such as informing them about acceptable business practices concerning the physical security

of hardware devices, software downloads, software evaluation copies, other areas. These policies must apply to both IT and end users as IT staff with administrator rights must be informed that it could create a risk in the same way that ends users could. In some organizations, for example in highly regulated industries, it will be easy to create a corporate culture to adhere to policies. However, other companies, such as engineering and IT companies will never succeed in controlling user behavior. At this level, costs and risks are visible because they can be scheduled annually. Moreover, the delays are modest, and the quality of the service increases. The company has confidence in IT, and end-users feel as though they have the resources to be effective.

- **Level 3: Optimised:** In the ITAM maturity model, the optimized level is the highest achievable level. Organizations have already solved many problems that prevent IT executives from being awake at night. The previous reactive issues have been resolved so that governance and policies are no longer a problem. Staffing will not be challenging as teams are already working together. At this level, the emphasis is placed on aligning the IT financial management provided by the ITAM data to enable a variety of strategic decision-making activities that are not necessarily related to ITAM but that support agility Business. Commercial agility is achieved when DevOps, SecOps (BMC, 2017) and ITAM Ops are all integrated processes and tools that share environmental data and real-time performance. In the Best case scenario, business units do not even realize that computing is taking place in the background. Achieving this level of agility requires a close alignment between business services through an operational ITAM and ITSM program. At this level, costs and risks are monitored and scheduled on a monthly basis, delays are short-term, and the quality of service is high. Business and IT are now linked with the same goals.

IT Asset Management Benefits

Today IT departments face many problems and expenses that could be mitigated by proper ITAM. Tracking the retirement rental assets is essential to know what assets the organization has, where they are and how they are preparing at any stage of their life cycle. Benefits of an effective IT Asset Management:

- Minimize the cost of maintenance
- Reduce system downtime

- Decrease hardware budgets
- Monitor warranty, recall, and lease information
- Prevent data breaches through proper disposal
- Potentially save or make money through disposal

IT Security Management

To manage and control the security management process to meet external/internal security requirements as it is found in SLAs, contracts, legislation and the company security policy” (Meziani & Saleh,). The ITSM/ITAM must offer an efficient but above all secure service. This component aims to assess vulnerabilities and patch management in heterogeneous computing environments. Also, this component enables you to establish and maintain the necessary security and the stability and performance of applications and systems. The control of this axis makes it possible to:

- Increase productivity and quickly evaluate information assets (hardware, software, processes, etc.) through a dynamic analysis of vulnerabilities and security risks.
- Be more serene by identifying vulnerabilities against standardized information sources.
- Monitor the situation using a single tool to find, analyze and download available patches.
- Improve system availability and user satisfaction by effectively remediating known vulnerabilities through targeting and automatic patch distribution.
- Vulnerability identification enables active scanning of computers to identify vulnerabilities in applications and operating systems against publishers’ information sources. Security bulletins can be an excellent solution for managing the vulnerability aspect of the company’s information assets. The security bulletins have critical information such as the relevant system platform, editor, application, criticality, date of publication, patch dependencies, etc. Thus allowing the console to sort them quickly.
- Updates of bulletins should regularly be made to ensure a high level of detection.

Also, there is a need for increased collaboration and cooperation between the IT security team and the IT operations team within an organization. In

many cases, these two IT groups within an organization are in contradiction. IT security is concerned about risks and threats, policy definition and environmental assessment, while IT operations, server administrator, network administrator, and office administration availability and performance, maintaining a stable environment, managing changes and not allowing all of this to disrupt availability and performance. IT security often leads to policies, recommendations, and deploys new technologies quickly in response to attacks and threats, sometimes forcing technology into the environment that may have management or performance issues.

IT Security Maturity Management Model (S3M)

The threat environment continues to evolve rapidly, and the volume of different malware is growing, increasingly being applied and web-based. To complicate the puzzle, your users are different. They bring things to the network and the information is just an application store and a credit card. The current approach to computer systems and security management must be more user-oriented (LANDESK, 2010).

Companies' efforts to improve security can motivate them to react and buy high-tech products that can make them more secure rather than more secure. The problem is that this proliferation of advanced attacks does not allow you to be more responsive. Taking a more proactive approach to security involves the deployment of multiple layers of integrated protection that stifle network violations. Table 5 indicates some of the trends of reactive organizations versus those that are more proactive or have more mature IT security.

The best approach is to ensure that your members of the information security team respond to new threats and your IT team member's process mature systems. Analysts Peter Firstbrook and Neil MacDonald of Gartner, Inc. : "A properly configured and corrected endpoint will be immune to the vast majority of malware attacks, which will allow security professionals

Table 5. Reactive\proactive mature IT security

Low-level security	Multiple point solutions
Multi-layered security	Integrated security solution
Inefficient use of IT resources	Processes that are reduced to minimal steps
Manual methods to quarantine threats	Automatic ways to isolate threats
IT Security manages all security processes	IT Operations manages known security processes while IT Security continues to monitor and investigate threats

to focus on attacks More sophisticated systems that are not dependent on malformed or vulnerable systems. IT organizations must prioritize security patches, especially for Internet-based applications, end-user applications that can run Java, browser and standard plug-ins (such as Java and Adobe Reader) and operating system. IT security professionals have a few choices available to drive their organizations towards more mature security solutions. They can continue to deploy point solutions and then try to manage them separately or computer operations operate them. They can implement point solutions, “tear, and replace” as they find more consolidated security solutions. Alternatively, they can get a solution that integrates with the IT workflow to manage endpoint devices and take advantage of multilevel integrated security. We propose a mature systematic approach to achieve an effective IT security management, as shown in Table 6. The path to security maturity requires a diversified range of layered endpoint protection, management and capabilities Defensive, all integrated and fully automated.

Agility Management

To take advantage of the digital age, companies realize that they need to deliver strategic responses more quickly and efficiently. This requires a pervasive agility throughout the enterprise. ITSM/ITAM teams are already focused on improving or constructing consistent, repeatable processes that reduce downtime and increase productivity (Robert, et al., 2016). Effective initiatives within the framework of the ITSM/ITAM can extend the delivery and management of business services beyond the areas of computing. Service management teams become an advisory model for the company, and your integrated, process-driven ITSM/ITAM enables agility that supports business strategy (Giudice, Christopher, Amy, & Ian, 2016).

By agile, we do not just mean “fast”, but it is a significant element. Agility in ITSM/ITAM is more a measure of responsiveness, and not just, how fast IT technicians process tickets or changes in version. Rather, true agility includes the entire IT team that solves service demands while respecting optimized labor costs. In short, real ITSM/ITAM agility is achieved by implementing intelligent processes that work smarter and more efficiently.

Transforming IT requires organizations to re-engaging IT processes - but too often re-engineering leads to frustration and failure. In most cases, IT organizations implement new processes and tools without taking into account the impact of changes in the organizational structure and the people involved.

IT Management Agility in Large Organizations

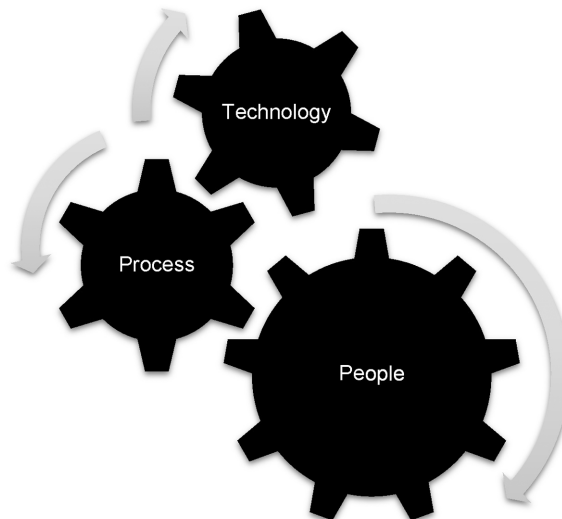
Table 6. Security maturity model

The maturity of capability building blocks		Level 1: Initial	Level 2: Basic	Level 3: Intermediate	Level 4: Advanced	Level 5: Optimizing
IT Service Security Management	Business continuity planning					
	IT Incident Management					
	Communication & Training					
	Security performance reporting					
IT Asset Security Management	Security budgeting					
	Resource effectiveness					
	Resource effectiveness					
	Tools & resources					
	Data identification & classifications					
Vulnerability and Risk Management	Access rights management					
	Security threat profiling					
	Security risk assessment					
	Security risk prioritization					
	Security risk monitoring					
	Data identification & classifications					
Compliance Management	Access rights management					
	Compliance control					
	Security assessment					
	IT services, processes, and systems comply with enterprise policies					

The implementation (or transition) of a DevOps development process (integration of both development, operational teams and processes) has proven to be a tool capable of reducing publication time; automation improved repetitive processes and a key element of Agile Development and Liberation. While agile development has led to increased focus and development of the DevOps model, DevOps is not changing at all. DevOps can (and should) be introduced and implemented in traditional development environments, where appropriate, and improvement can be measured. However, DevOps is not a unique technology, process or tool. Adopting DevOps requires changes in the way teams are structured, how responsibilities are shared, and the need to integrate and deliver services that enable teams to succeed.

In parallel with the development solutions and processes, ITSM/ITAM plays a vital role in supporting DevOps practices and objectives such as incident management, application deployment, and performance management, to name a few. The conception and implementation of new agile ITSM/ITAM are a challenge. The proposed DevOps model connects people, process, and technology to ensure continuous improvement, as shown in Figure 6.

Figure 6. DevOps agility: Aligning people, technology, and process for continuous improvement



Process Management

While technology management has been the primary element of IT, most IT organizations realize that poor service delivery pretty much with technology. For example, the best technology is not useful if a service offer fails due to process-related issues shown in Table 7.

IT should be prepared to restore services as quickly as possible in the event of a problem. Well-defined roles and responsibilities are essential for service disruptions. Anyone involved in the delivery and support of the service must perform without confusion or delay. This ability can be the critical difference between the success and failure of an IT organization trying to establish credibility as a service provider. These situations are examples of process problems. Successful commercial success is complicated to achieve until they are processed.

Table 7.

<p>Unscheduled Changes Unprogrammed - and therefore uncontrolled</p>	<p>Changes occur in the production environment due to clear and undocumented computer processes. Problems in the change management process lead to false starts, multiple withdrawals, duplicate efforts, periodic work stoppages, prolonged repair time intervals, and increased client anxiety and frustration. For a service provider, these problems can be catastrophic. Customers require predictability of delivery time, quality, and service performance, but IT organizations cannot provide it if the service delivery environment is unreliable.</p>
<p>Vague process triggers Triggers for IT processes</p>	<p>For example, software distribution is poorly defined. As a result, IT personnel inadvertently start a process at different points, resulting in inconsistent and unreliable service delivery. This type of process problem can have a grave impact on customer satisfaction and avoid repeating business, and it communicates that IT cannot commit to meet service levels.</p>
<p>Undefined or nonexistent process links</p>	<p>The links between IT processes are unclear or non-existent, making it impossible to capture information and share among several processes related to agility, flexibility and increased responsiveness of enterprises. Link issues can lead to delays in already rigorous production schedules, low customer satisfaction, missed customer commitments and, ultimately, loss of revenue. Customers are now expecting a quick response to their business transactions, whether or not they are used. To meet their needs, IT must be able to capture information and share it among related processes. These links allow business agility and flexibility customer's demand.</p>
<p>Unreliable roles and responsibilities IT employees responsible for a process</p>	<p>Such as incident management or problem management - are unclear about their roles and are not evaluated on a regular basis, which contributes to difficulties in attributing the Responsibility when problems arise.</p>

People

Improved processes are useless without people. Nevertheless, the people component of IT refers to more than a mere understanding of how process re-engineering and process management affects IT, staff. It also refers to skill sets, attitudes, and the new roles and responsibilities team must assume to be successful. Each of these people aspects must be transformed for IT organizations to evolve from technology to service providers. IT staff skills must change in support of new or modified jobs that result from process engineering and changing or improving skills requires education and training. However, proper performance of new skills alone does not necessarily result in successful IT transformation. Attitudes must also be transformed so that the entire IT department becomes more customer-focused, service-oriented, and aligned with the business goals of the organization (Table 8). In practical terms, this means IT organizations must:

- View consumers of their services as customers
- Temper their traditional inward perspective and start looking outward
- Expand their focus on technology to include a focus on service solutions
- Move away from isolated, ad hoc processes and develop business-justified, streamlined IT processes
- Implement measurable, accountable processes
- Balance in-house solution development with outsourcing
- Design and implement integrated, end-to-end IT processes, avoiding process silos
- Utilize new process improvements to support a proactive approach
- Define and develop service-oriented organizational structures, roles, and responsibilities
- Enhance traditional IT system skills with customer-focused skills.

Achieving these changes in skills and attitudes throughout an IT organization requires a well-defined educational program that addresses processes and technology. In most cases, organizations benefit from hiring a consultant who understands these needs and can develop a tailor-made plan. Once new processes are implemented, and there are measurable and reportable outcomes, people's attitudes move toward service and customer focus. However, the tone set by IT leadership also has a significant impact on staff attitudes.

IT Management Agility in Large Organizations

Table 8. New skills and attitudes required for successful IT transformation

From		To
Users	→	Customer
Inward-looking	→	Outward-looking
Technology focus	→	Process focus
Ad hoc processes	→	Rationalized, streamlined processes
Best efforts	→	Measured, accountable processes
Entirely in-house	→	Balanced in-/outsourcing
Fragmented, silos	→	Integrated, end-to-end
Reactive	→	Proactive
Operations manager	→	Service management
System skills	→	Listening skills

IT processes Agility also requires new roles and responsibilities. Attempting to introduce new or significantly improved IT processes without addressing the roles, responsibilities, metrics, and underlying job descriptions can result in a bad performance, frustrated staff, and potential failure. For IT transformation to be successful, roles and responsibilities need to change to reflect new processes and service priorities, and these changes should affect the entire IT organization.

Technology

Making new or improved IT processes function smoothly often requires significant changes to existing technologies as well as incorporating new technologies into the existing IT environment. IT also needs process-enabling technologies with special tools to automate processes and simplify the inter-process integration and communications for managing IT services enterprise-wide.

In addition to process-enabling technologies, other tools may be required for an overall ITSM/ITAM solution, such as tools that:

- Allow companies to view their Internet infrastructure, simulate, and monitor business activity
- Monitor the performance of Web sites and improve the customer experience

- Monitor and analyze telecom service impact and quality
- Provide timely and accurate service reporting, or create portal views that provide customers with visibility into their services

To simplify implementation, reduce costs and improve processes, IT organizations must identify tools that require minimal customization. For example, consider the benefits of purchasing a change management system that is already integrated with configuration management, incident management, support system, and service management systems. As change orders are processed, the past, current, and future IT infrastructure data can be retrieved automatically from configuration management and updates. Data from recent incidents can be collected immediately, significantly reducing review and approval time for a particular change. The same data, when also available for problem management, allows specialists to analyze trends and avoid future interruptions to the service. At the same time, change management and incident management personnel can access problematic data to improve quality and decision-making. Support staff can quickly determine the levels of service applied and the escalation parameters for callers, which improves customer satisfaction.

When evaluating technologies, you will want to compare the off-box features of each option carefully. It is also important to take into consideration the ease with which the technologies for creating processes can be integrated into the enterprise IT environment. The integration can range from the insertion of an entry on a menu bar to a large-scale data exchange between applications. IT organizations need to determine their needs and select a product that allows for the desired level of integration and meets the cost criteria. A common trap in choosing a process automation tool does not properly evaluate and prioritize business needs before starting the selection process. For example, IT organizations may need to set up an excellent support service and improve the integration of IT processes. Many companies attempt to evaluate technological options by considering both, comparing a mix of point-of-care solutions with computer process integration solutions. Unfortunately, few, if any, integrated IT process tools have a help desk component that can compete with an excellent support service solution. On the other hand, the choice of a less feature-rich desktop solution can be easily offset by the various benefits of an integrated IT services management solution, which will facilitate the transformation of IT processes to multiple levels.

Agility Maturity Model Based on DevOps

To understand the DevOps maturity of the core development and IT operations processes, we propose a proven DevOps maturity model based on a return to the experience of the adoption of DevOps model of agility in their business strategy to accelerate innovation and meet market demands. This model looks at DevOps from three viewpoints IT service, process, assets, IT automation, and IT collaboration, and spans a series of clearly defined states on the path to an optimized DevOps ITSM/ITAM environment. The DevOps maturity model described in Figure 7 below represent a roadmap to achieve organization's maturity level regarding ITSM/ITAM standardization, IT automation tools, IT collaboration approaches, and end IT user security management, along with insights into your opportunities for continuous IT service operations and organizational change improvement.

USE CASE

In this part, we will study a case of application of our model to a company, and the gain made on the strategic level and decision-making. We propose to measure the maturity of the ITSM/ITAM of the organization and set up our benchmark to improve IT governance through the proposed global, practical and agile ITSM/ITAM model.

We conducted a study of the practices used by companies to manage the ITSM/ITAM service center. This study is based on a questionnaire drawn up in a sample of 10000 IT professionals (Director, IT Manager, IT practical).

The objective is to have a return experience about the IT services and assets management best methods and practices. To measure the contribution of our proposed framework on the company's IS performance. This model has been implemented in the IT department of a port sector organization since the year 2014. We will discuss in this part the results of this implementation and the adoption of the proposed practical and agile ITSM/ITAM approaches and solutions that are both ITIL compliant and also supports the continued IT change management and improvement. Figure 8 describes the architecture of the proposed IT Service Center for the organization.

Figure 7. Devops ITSM/ITAM Maturity model for continues organization’s measure and improvement

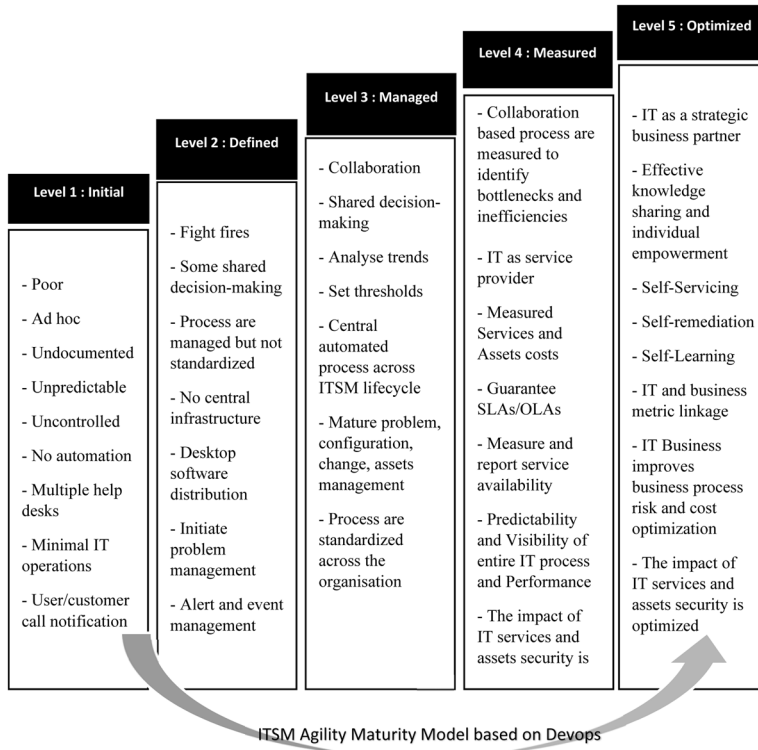
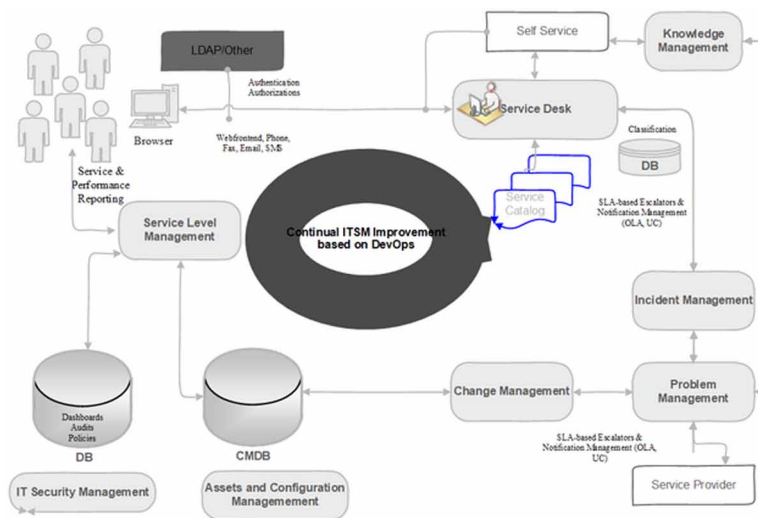


Figure 8. The proposed design of the agile and secure IT service center



Methodology

To be able to meet the requirements of the proposed ITSM/ITAM Framework, all employees must feel concerned and involved. To this end, the quality department has undertaken a series of strategic actions. These activities are planned following an agile model based on DevOps. Inspired by Deming wheel and DevOps, we organize the reports into four phases DDAO: Discover Do, Act, and Optimize, as shown in Table 9. Our goal is to develop a quality approach for continuous IT improvement. Starting with the auditing of all the functional and practical aspects of the management of the organization's services and the desired need, including the implementation of a roadmap for the desired organizations levels of maturity regarding management of services, assets and IT security. We define an agile approach based on the proposed model DevOps, to guarantee a continuous improvement of the processes, services, security and organization, and contribution to the business of the organization.

Data Collection

The questionnaire was carried out in several stages. A first version has been developed to take into account the different theoretical assumptions. This first version has been tested with IT service managers and consultants. This pre-test allowed rephrasing some questions to improve the comprehension of the questionnaire and to improve the quality of the given answers. In the end, the questionnaire consists of 100 questions divided into four topics: IT service management maturity, IT asset management maturity, IT security management maturity and IT agility maturity level.

Table 9. Continual quality improvement

DISCOVER	DO	ACT	OPTIMIZE
Vision and Strategy	Assessment	Organization	Performance Management
Auditing	Strategic Plan	Processes	Benchmarks
Key Performance Indicators	Roadmap	Tools And Technology	Continuous Improvement

Table 10. Organization staff and turnover

	Year	Frequency
Size of the Company (# of Employees)	2017	More than 1,200
Position	Senior Executives	366
	Executives	95
	Supervisory Officers	415
	Qualified non-supervisory	146
	Non-supervisory	79
<i>Evolution of Turnover and Revenue of the Company for the last 5 years in \$</i>	2012	More than \$1,5 million
	2013	Less than \$3 million
	2014	More than \$1,7 million
	2015	More than \$1,5 million
	2016	Less than \$2 million
	2017	More than \$2 million

Table 11. Participants' demographics

Participants	Frequency	Percent
Male	68	68,42%
Female	36	31,58%
Top manager personnel	17	14,91%
Senior Manager	23	20,18%
IT Manager	7	6,14%
Consultant/Engineer/Analyst	13	11,40%
IT Technical Staff	19	16,67%
Helpdesk Technician	7	6,14%
Quality Assurance / Quality Control	15	13,16%
Other entities staff	13	14,91%

Data Analysis

We used the questionnaire in Table 12 (Appendix) to drive data analysis. The questionnaire includes the different objectives and controls of the proposed ITSM/ITAM framework. We attempted to validate each answer through the developed maturity software that was used to automate the process and determine the maturity score. The treatment consists of calculating a weighted average of the scores obtained based on the selected responses and the coefficient of efficiency of each function in the organization. Questions

also changed from Yes/No to five options related to maturity levels as shown in Figure 9. The toolbox worksheet contains contextual answers for each question in the assessment. The formulas in the toolbox will average the answers to calculate the score for each practice. The score is a numerical result (zero to five or expressed as a percentage) representing the maturity level of the audited ITSM/ITAM.

Discover

The following section presents the part of the empirical study that concerns and identifies the measuring system of IT in the organization. During the empirical study, different possibilities in measuring and comparing the KPIs in different groups were found. In the following section, we will present measuring operations and visualization of measurements and auditing of IT services and security in the organization. IT managers described that there are different parts of ITIL that are incorporated in the fields of IT Support, Service desk SLA's, Incident and Problem management and Deployment fields. The most important parameters to measures are targeting Time Deliveries in different channels such as General Service management of core system functions, Business projects, Activities, Operational maintenance, and Admin. Another aspect that could be measured is Service improvement by providing surveys based on a yearly basis (on process and maintenance object level) to improve and monitor the overall performance of the systems.

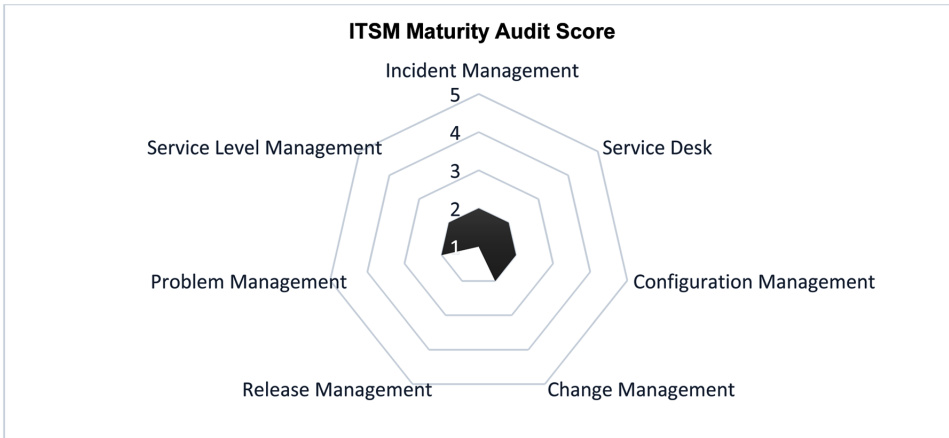
ITSM Audit Score

We conducted an audit of the organization's ITSM practices. In order to define the current levels of maturity and to define the desired level to be attained by the organization. The maturity score 1 indicates the initial level (ad hoc), and the score 5 indicates the high score of maturity level (optimized). The Figure 10 below shows the current ITSM maturity level (2. Defined)

Figure 9. Assessment score



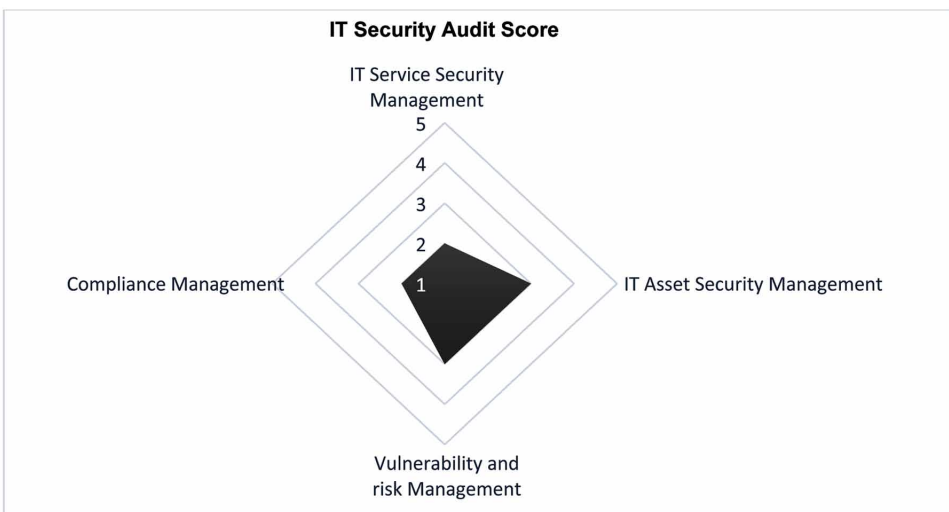
Figure 10. ITSM Maturity score



IT Security Audit Result

Based on the model of security maturity on Table 6. We audit endpoint security of the organism that runs between the basic and intermediate level. Our objective is to achieve an improved level of ITSM security and to be part of the overall governance of the organization's information security. The results of the audit are illustrated in Figure 11.

Figure 11. IT security audit score



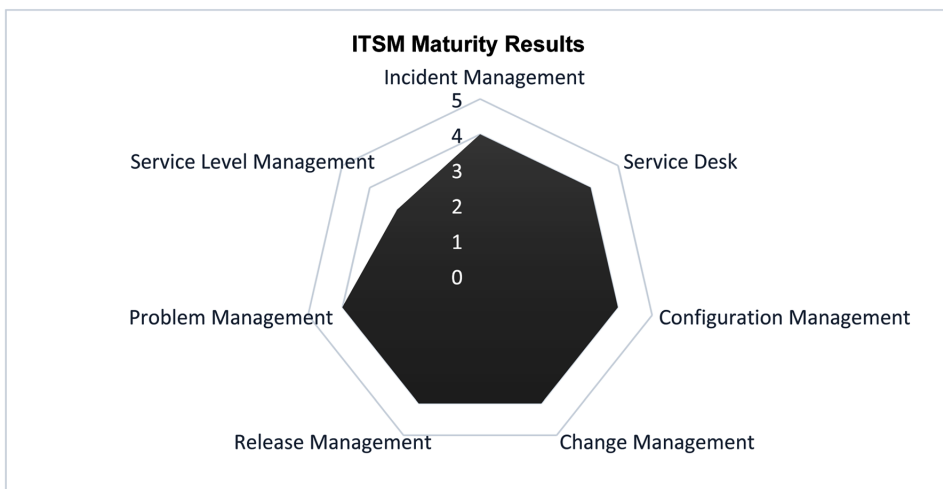
The Practical Framework to Enhance ITSM Efficiency

In section 4, we have proposed different feedbacks about the system performance without modifying the new solutions for the future model. In this section, it would be helpful to be able to provide experimental model behavior, which has been missing in the Service Quality of IT Service Management process with some suggestion to improve different approaches, which we have evaluated. To conclude the issue, we could say that organizations should seriously take the advantage of learning from the system performance and should reduce the appropriate Incident management because successful approach and proper IT service management plan could make the difference between the organization's continued existence and sudden death. The suggested framework is a structured approach to increase the perception of ITSM efficiency and to reduce incident management in new start-up companies. In this part, we discuss the axes of improvement referring to the results of the empirical study and interviews with the IT managers in different areas of the ITSM.

IT Service Management

In this part, we will discuss the improved points treated in terms of IT service management. The adoption of the proposed ITSM framework described in section 3 help the organization to increase the level of ITSM maturity to level 4: managed as shown in Figure 12.

Figure 12. ITSM Maturity score after implementation



User expectations have changed and the IT department has to develop other ways of communicating with them. The goal is to provide IT Service Management with a tool to anticipate their requests, optimize productivity, reduce downtime, and have all the necessary ITSM processes, including incident management, problem management, Changes, requests, self-service, as well as SLA management, etc. The proposed solution fits easily into IT operations.

- Control of the support center with fundamental processes
- Improved service and support performance, and reduced unforeseen costs and business risks.
- Support center solution is easy to use and administer
- IT administrators can easily configure, design and modify the support center system. IT teams can configure it without coding to meet the changing needs of the enterprise and achieve faster profitability without disrupting users.
- Improved user satisfaction through the self-service portal: Secure self-service functions, available anywhere and all the time enable end users to log and resolve their own IT incidents, and display relevant information. The service catalog allows the end user to view and use the services for which they have rights. Automatically provide and maintain services, linking them to the policy and objectives of the IT department.
- Improved visibility of operations through reports and dashboards: Quickly evaluate your performance against the company's goals, for continuous improvement. Easily create or configure multilevel reports based on the metrics used to demonstrate the value of IT Service Management (ITSM) for the enterprise. Dashboards with cascading analysis functions to trend charts based on KPIs to provide context for decision-making and planning. The benefits of the adoption of the practical ITSM framework are:
 - 95 percent success rate on SLAs
 - Reports meet auditor requirements
 - 50 percent reduction in end-user calls
 - Data confirms cost-cutting decisions
 - Improved IT asset management and cost control
 - Set up an agile approach to deal with the different changes in the SI
 - Improving the management of the security of IT services

IT Management Agility in Large Organizations

- Implement a continuous improvement strategy DDAO (Discover, Do, Act, Optimize).

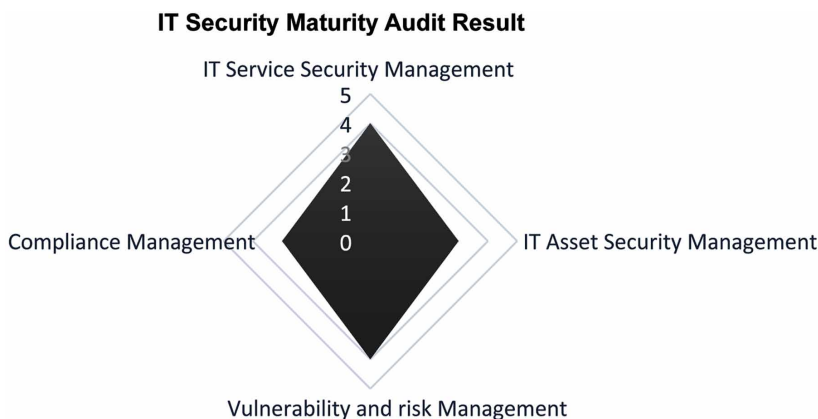
IT Security Management

Organized cybercrime has only one target: user data. Data protection against the most complex threats. After auditing this axis, it appears that this component is not supported in the IT Service Management process, and the management of security incidents is not supported. We proposed to implement a security management solution based on the model defined in section 3, to provide better visibility of risks, to facilitate compliance with current regulations and to improve your overall level of security. Figure 13 illustrates the results of IT level of Security Maturity after implementation.

Act

This step will evaluate the decisions taken and the approach was taken. The quality department and management will study the results and judge the relevance of the decisions made. Moreover, this stage is required to reduce the gaps and dysfunctions deployed during each review or audit. The planned management review each year takes into account the steps taken during the year or the last six months in trying to define opportunities for improvement. We exploit the DevOps approach to set up this step. DevOps brings fundamental changes to how application and execution teams interact and execute processes. It requires changes in technology, processes, and culture, and changes at this

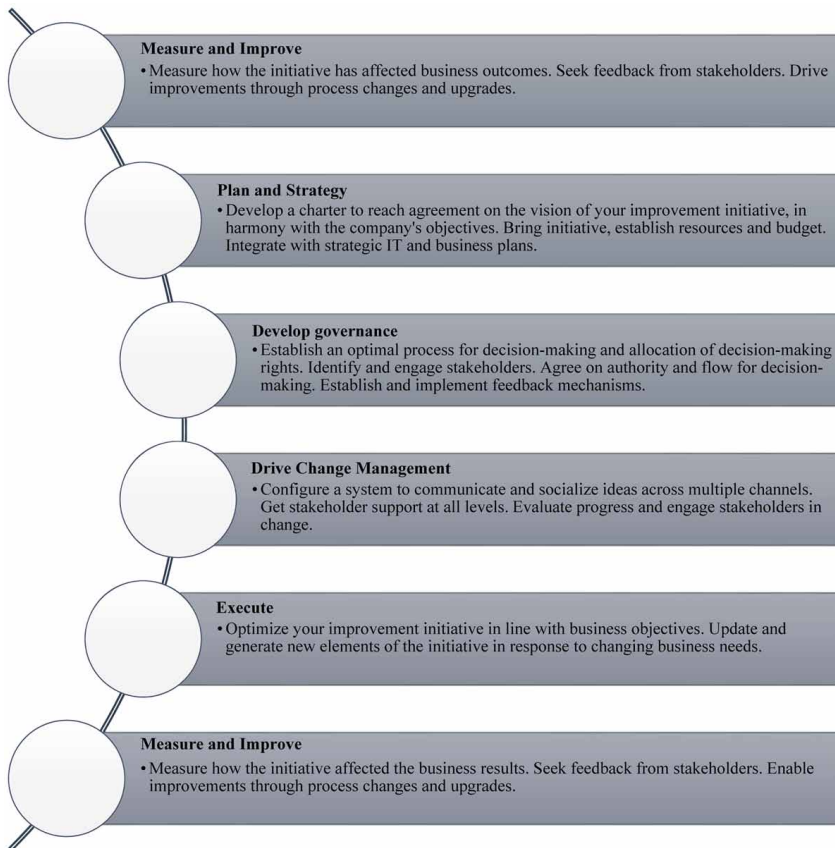
Figure 13. IT security maturity audit result after implementation



level can be difficult to resolve unless they are addressed in a systematic way. We measure the organization agility level by the proposed DevOps ITSM Maturity model for continues organization’s measure and improvement. The organization’s level of agility is initial; our objective is to orient the ACT part towards an agile approach, in order to ensure a delicate change management and consequently a continuous improvement by supporting people, process and technology drivers. To creating an agile IT service/assets center that delivers quicker resolutions, increases user satisfaction and evolves with rapidly changing technologies, we suggest following these steps described in Figure 14.

The results obtained can be improved agile by adopting our agile approach based on DevOps. This approach will allow any organization to measure, control and manage IT services, asset and endpoint security costs and process.

Figure 14. Devops continues IT improvement



Optimize

The most important thing that organizations adopt agile practices is that there is no end to the journey and that they need to continuously improve to remain leaders. Customers always expect more, and competitors will always be there to deliver it if you don't do it first. Remaining a leader requires adapting to customer feedback and continually improving products and practices, and recognizing when it's time to pivot. New metrics are defined to measure and manage improvement, as well as value delivered.

Benefices of the Proposed Agile ITSMA/ITAM After Implementation

User expectations have changed, and the IT department has to develop other ways of communicating with them. The goal is to provide IT Service Management with a tool to anticipate their requests, optimize productivity, reduce downtime, and have all the necessary ITSM processes, including incident management, problem management, Changes, requests, self-service, as well as SLA management, etc. The proposed solution fits easily into IT operations.

- Control of the support center with fundamental processes
- Improved service and support performance, and reduced unforeseen costs and business risks.
- Support center solution is easy to use and administer
- IT administrators can easily configure, design and modify the support center system. IT teams can set up it without coding to meet the changing needs of the enterprise and achieve faster profitability without disrupting users.
- Improved user satisfaction through the self-service portal: Secure self-service functions, available anywhere and all the time enable end users to log and resolve their own IT incidents, and display relevant information. The service catalog allows the end user to view and use the services for which they have rights. Automatically provide and maintain services, linking them to the policy and objectives of the IT department.
- Improved visibility of operations through reports and dashboards: Quickly evaluate your performance against the company's goals, for

continuous improvement. Easily create or configure multilevel reports based on the metrics used to demonstrate the value of IT Service Management (ITSM) for the enterprise. Dashboards with cascading analysis functions to trend charts based on KPIs to provide context for decision-making and planning. The benefits of the adoption of the practical ITSM/ITAM framework are:

- 95 percent success rate on SLAs
- Reports meet auditor requirements
- 50 percent reduction in end-user calls
- Data confirms cost-cutting decisions
- Improved IT asset management and cost control
- Set up an agile approach to deal with the different changes in the SI
- Enhance the management of the security of IT services
- Implement a continuous improvement strategy DDAO (Discover, Do, Act, Optimize).

CONCLUSION

In the age of digitization, the world is evolving at a constant pace. Companies need to respond to changing conditions and often agility is the only guarantee of survival. Globalization means that there is more competition. The life cycle of products is shorter than ever. A disruptive technology can change markets overnight.

The company faces challenging challenges in maintaining security and compliance while achieving its business objectives, complying with current regulations, and managing staff and technology. We understand that your IT staff must be able to react quickly to changing business needs while maintaining your existing infrastructure. We also know that the management objective so often quoted, “Doing more with less” is not only a goal, it is a corporate commitment. In this work, we propose a global model of strategic agility for the management of IT services. This framework surpasses the limitations of existing methods/referential and meets the needs of international standards in terms of flexibility and agility in order to improve ITSM processes.

The next chapter will discover the role of Cloud Computing in improving IT agility by presenting recent studies in the literature on IS and IT management.

REFERENCES

- Allen, B., & Boynton, R. (1991). Information Architecture: In Search of Efficient Flexibility. *MIS Quarterly*.
- Ang, A. (2014). *Asset management: A systematic approach to factor investing*. Oxford University Press. doi:10.1093/acprof:oso/9780199959327.001.0001
- Bartolini, S. (2006). IT service management driven by business objectives An application to incident management. *IEEE/IFIP Network Operations and Management Symposium NOMS*.
- Baskerville, R., & Pries-Heje, J. (2004). Short cycle time systems development. *Information Systems Journal*, 14(3), 237–264. doi:10.1111/j.1365-2575.2004.00171.x
- Beck, K. (1999). *Extreme Programming Explained: Embrace Change*. Addison-Wesley.
- Bhatt, G., Emdad, A., Roberts, N., & Grover, V. (2010). Building and leveraging information in dynamic environments: The role of IT infrastructure flexibility as enabler of organizational responsiveness and competitive advantage. *Information & Management*, 47(7–8), 341–349. doi:10.1016/j.im.2010.08.001
- BMC. (2017). Enterprises re-engineer security in the age of digital transformation (White Paper). *Forbes Insights*.
- Boar, B. (1998). Redesigning the IT Organization for the Information Age. *Information Systems Management*, 15(3), 23-30.
- Börjesson, A., Martinsson, F., & Timmerås, M. (2006). Agile Improvement Practices in Software Organizations. *European Journal of Information Systems*, 15(2), 169–182. doi:10.1057/palgrave.ejis.3000603
- Broadbent, M., Weill, P., & St.Clair, D. (1999). The Implications of Information Technology Infrastructure for Business Process Redesign. *Management Information Systems Quarterly*, 23(2), 159–182. doi:10.2307/249750
- Brooks. (2006). *Metrics for IT service management*. Zaltbommel: Van Haren Publishing.
- Butler, B., & Gray, P. (2006). Reliability, Mindfulness, and Information Systems. *Management Information Systems Quarterly*, 30(2), 211–224. doi:10.2307/25148728

Byrd, T., & Turner, D. (2000). Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct. *Journal of Management Information Systems*, 17(1), 167–208. doi:10.1080/07421222.2000.11045632

Ciborra, C. (1992). From Thinking to tinkering: The grassroots of IT and strategy. *The Information Society*, 8, 297–309. doi:10.1080/01972243.1992.9960124

Clark, C., Cavanaugh, N., Brown, C., & Sambamurthy, V. (1997). Building Change-Readiness Capabilities in the IS Organization: Insights From the Bell Atlantic Experience. *Management Information Systems Quarterly*, 21(4), 425–455. doi:10.2307/249722

Conboy, K. (2009). Agility from first principles: Reconstructing the concept of agility in information systems development. *Information Systems Research*, 20(3), 329–354. doi:10.1287/isre.1090.0236

Das, Z., Zahra, S. A., & Warkentin, M. E. (1991). Integrating the Content and Process of Strategic MIS Planning with Competitive Strategy. *Decision Sciences*, 22(5), 953–984. doi:10.1111/j.1540-5915.1991.tb01902.x

Duane, L., & Charlie, S. (2016). *Reducing the cost of test through strategic asset management*. IEEE Autotestcon.

Duncan, N. (1995). Capturing Flexibility of Information Technology Infrastructure: A Study of Resource Characteristics and Their Measure. *Journal of Management Information Systems*, 12(2), 37–57. doi:10.1080/07421222.1995.11518080

Dybå, T., & Dingsøyr, T. (2008). Empirical Studies of Agile Software Development. *Systematic Reviews*, 50(9–10), 833–859.

Fink, L., & Neuman, S. (2009). Exploring the perceived business value of the flexibility enabled by information technology infrastructure. *Information & Management*, 46(2), 90–99. doi:10.1016/j.im.2008.11.007

Gebauer, J., & Schober, F. (2008). Information system flexibility and the cost efficiency of businessProcesses1. *Journal of the Association for Information Systems*, 7(3), 122–146. doi:10.17705/1jais.00084

Gene, K., Jez, H., Patrick, D., & John, W. (2016). *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations*. IT Revolution Press.

Gerth, A., & Rothman, S. (2007). The Future IS Organization in a Flat World. *Information Systems Management*, 24(2), 103–111. doi:10.1080/10580530701221007

Giudice, D. L., Christopher, M. A., Amy, H., & Ian, M. (2016, 03 30). *Agile And DevOps Adoption Drives Digital Business Success*. Cambridge, UK: Forrester Research. Retrieved from Transforming IT organizations into service providers: www.hp.com/hps/itsm

Goldman, S. N. (1995). *Agile Competitors and Virtual Organizations: Strategies for Enriching the Customer*. New York: Van Nostrand Reinhold.

Gupta, P. (2008). Automating ITSM Incident Management Process. *International Conference on Autonomic Computing*.

Hank. (2006). ITIL: What It Is And What It Isn't. *Business Communications Review*.

Hewlett Packard. (2016). *HP DevOps*. Retrieved from <https://www.hpe.com:https://saas.hpe.com/fr-fr/software/devops-solutions>

Holmqvist, M., & Pessi, K. (2006). Agility Through Scenario Development and Continuous Implementation: A Global Aftermarket Logistics Case. *European Journal of Information Systems*, 15(2), 146–158. doi:10.1057/palgrave.ejis.3000602

Hong, W., Thong, J. Y., Chasalow, L. C., & Dhillon, G. (2011). User acceptance of agile information systems: A model and empirical test. *Journal of Management Information Systems*, 28(1), 235–272. doi:10.2753/MIS0742-1222280108

ISO/IEC 20000. (2010). *ISO/IEC 20000 Information Technology*. ISO/IEC 20000.

Joachim, N., Beimborn, D., & Weitzel, T. (2013). The influence of SOA governance mechanisms on IT flexibility and service reuse. *The Journal of Strategic Information Systems*, 22(1), 86–101. doi:10.1016/j.jsis.2012.10.003

Jurison. (1996). Toward more effective management of information technology benefits. *The Journal of Strategic Information Systems*, 263–274.

Kumbakara, N. (2008). Managed IT services: The role of IT standards. *Information Management & Computer Security*, 16(4), 336–359. doi:10.1108/09685220810908778

Kumbakara. (2008). Managed IT services: the role of IT standards. *Information Management & Computer Security*.

Lacity, M., Willcocks, L., & Feeny, D. (1995). IT Outsourcing: Maximize Flexibility and Control. *Harvard Business Review*, 73(3), 84–93.

Lahtela, J. (2010). Implementing an ITIL-Based IT Service Management Measurement System. *Fourth International Conference on Digital Society*.

LANDESK. (2010). *Achieving Security Maturity* (White Paper). Retrieved from LANDESK: <http://landesk.avocent.com/WorkArea/downloadasset.aspx?id=5232>

Lee, G., & Xia, W. (2005). The Ability of information System Development Project Teams to Respond to Business and Technology Changes: A Study of Flexibility Measures. *European Journal of Information Systems*, 14(1), 75–92. doi:10.1057/palgrave.ejis.3000523

Lee, O., Banerjee, P., Lim, K., Kumar, K., Hillegersberg, V., & Wei, J. (2006). Agility in Globally Distributed System Development. *Communications of the ACM*, 49(10), 49–54. doi:10.1145/1164394.1164419

Luftman. (2003). Assessing IT-Business alignment. *Information Systems Management*, 9-15.

Lyytinen, K., & Rose, G. M. (2006). Information System Development Agility as Organizational Learning. *European Journal of Information Systems*, 15(2), 183–199. doi:10.1057/palgrave.ejis.3000604

Markus, M., & Benjamin, R. (1996). Change Agency – The Next IS Frontier. *Management Information Systems Quarterly*, 20(4), 385–407. doi:10.2307/249561

Marrone, K., & Kolbe, L. M. (2011). Uncovering ITIL claims IT executives' perception on benefits and Business-IT alignment. *Information Systems and e-Business Management*, 9(3), 363–380. doi:10.1007/10257-010-0131-7

McAvoy, J., Nagle, T., & Sammon, D. (2013). Using mindfulness to examine ISD agility. *Information Systems Journal*, 23(2), 155–172. doi:10.1111/j.1365-2575.2012.00405.x

McCann, J., Selsky, J., & Lee, J. (2009). Building Agility, Resilience and Performance in Turbulent Environments. *People and Strategy*, 32(3), 44.

McNaughton, R., Ray, P., & Lewis, L. (2010). Designing an evaluation framework for IT service management. *Information & Management*, 47(4), 219–225. doi:10.1016/j.im.2010.02.003

Meade, L. M. (1997). Method for analyzing agility alternatives for business processes. In *Industrial Engineering Research - Conference Proceedings* (pp. 960-965). IIE.

Mesquida. (2012). IT Service Management Process Improvement based on ISO/IEC 15504: A systematic review. *Information and Software Technology*.

Meziani, S. (2010). E-government: ITIL-based service management case study. *The 12th International Conference on information integration and web-based applications & services*.

Mior. (2008). *The importance of ITSM. Malaysian Business*. Kuala Lumpur: New Straits Times Press.

Nicolett, M. (2010). *Best Practices in IT Security and IT Operations Integration. Gartner Security & Risk Management Summit*. Gartner.

Overby, E., Bharadwaj, A., & Sambaurthy, V. (2006). Enterprise Agility and the Enabling Role of Information Technology. *European Journal of Information Systems*, 15(2), 120–131. doi:10.1057/palgrave.ejis.3000600

Parger, K. (1996). Managing for Flexibility. *Information Systems Management*, 13(4), 41–44. doi:10.1080/10580539608907015

Park, K. (2008). The Study on the Maturity Measurement Method of Security Management for ITSM. *Proceedings of the 2008 International Conference on Convergence and Hybrid Information*. 10.1109/ICHIT.2008.251

Porter. (1996). What is strategy. *Harvard Business Review*.

Ramesh, B., Mohan, K., & Cao, L. (2012). Ambidexterity in agile distributed development: An empirical investigation. *Information Systems Research*, 23(2), 323–339. doi:10.1287/isre.1110.0351

Reich, B., & Benbasat, I. (2000). Factors That Influence the Social Dimension of Alignment between Business and Information Technology Objectives. *Management Information Systems Quarterly*, 24(1), 81–113. doi:10.2307/3250980

Richards, C. (1996). Agile manufacturing: beyond lean. *Production & Inventory Management*, 60-4.

Robert, H., Isabell, S., Kiess, O., Ingo, B., Sacha, M., & Bradley, L. (2016). *IT Service Management for DevOps*. Retrieved from IBM: <https://www.ibm.com/developerworks/community/files/form/anonymous/api/library/42529e82-173a-4f45-805b-93d9eb35ffa6/document/19b71c8c-1675-4727-a3ab-b259ba1d49e6/media/ITSM%20Reference%20Architecture%20-%20DevOps%20-%20Whitepaper.pdf>

Rockart, J. F., Earl, M., & Ross, J. (1996). Eight Imperatives for the New IT Organization. *Sloan Management Review*, 38(1), 43–55.

SANS Institute. (2009). *The Top Cyber Security Risks*. Retrieved from SANS Institute: <http://www.sans.org/top-cybersecurity-risks>

Sarker, S., & Sarker, S. (2009). Exploring agility in distributed information systems development teams: An interpretive study in an offshoring context. *Information Systems Research*, 20(3), 440–461. doi:10.1287/isre.1090.0241

Schmidt, C., & Buxmann, P. (2011). Outcomes and success factors of enterprise IT architecture management: Empirical insight from the international financial services industry. *European Journal of Information Systems*, 20(2), 168–185. doi:10.1057/ejis.2010.68

Schwaber, K. (2004). *Agile Project Management with Scrum*. Microsoft Press.

Scott, J. (2007). Mobility, Business Process Management, Software Sourcing, and Maturity Model Trends: Proposition for the IS Organization of the Future. *Information Systems Management*, 24(2), 139–145. doi:10.1080/10580530701221031

Sharp, J., Irani, Z., & Desai, S. (1999). Working towards agile manufacturing in the UK industry. *International Journal of Production Economics*, 62(1-2), 155–169. doi:10.1016/S0925-5273(98)00228-X

Sia, S. K., Koh, C., & Tan, C. X. (2008). Strategic maneuvers for outsourcing flexibility: An empirical assessment. *Decision Sciences*, 39(3), 407–443. doi:10.1111/j.1540-5915.2008.00198.x

Silva Molina, L. F. (2005). How to Identify and Measure the Level of Alignment between IT and Business Governance. *Proceedings of the PICMET*.

Stettina, J. C., Kroon, & Egbert. (2013). Is there an agile handover? an empirical study of documentation and project handover practices across agile software teams. In *Engineering, Technology and Innovation (ICE) & IEEE International Technology Management Conference, 2013 International Conference on* (pp. 1-12). IEEE.

Tan, C.-S. (2009). Implementing IT service management: A case study focussing on critical success factors. *Journal of Computer Information Systems*, 1–12.

Tanriverdi, H., Arun, R., & Venkatraman, N. (2010). Research Commentary: Reframing the Dominant Quests of IS Strategy Research for Complex Adaptive Business Systems. *Information Systems Research*, 21(4), 822–834. doi:10.1287/isre.1100.0317

Tiwana, A., & Konsynski, B. (2012). Complementarities between organizational IT architecture and governance structure. *Information Systems Research*, 288–304.

Truex, D., Baskerville, R., & Klein, H. (1999). Growing Systems in Emergent Organizations. *Communications of the ACM*, 42(8), 117–123. doi:10.1145/310930.310984

Uebernickel, B.-S. Z. (2006). Service-Engineering: A process model for the development of IS services. *Proceedings of the European and Mediterranean Conference on Information Systems (EMCIS)*.

van Bon, E. (2007). *Foundations of IT Service Management based on ITIL v3*. Van Haren Publishing.

van Grembergen, H. (2009). *COBIT as a Framework for Enterprise Governance of IT*. Boston: Springer US.

Vernadat, F. (1999). Research agenda for agile manufacturing. *International Journal of Agile*, 1(1), 37–40.

Volberda, H. (1996). Towards the flexible form: How to remain vital in hypercompetitive environments. *Organization Science*, 7(4), 359–387. doi:10.1287/orsc.7.4.359

Volberda, H., & Rutges, A. (1999). FARSYS: A Knowledge-based System for Managing Strategic Change. *Decision Support Systems*, 26(2), 99–123. doi:10.1016/S0167-9236(99)00023-8

Wang, X., Conboy, K., & Pikkarainen, M. (2012). Assimilation of agile practices in use. *Information Systems Journal*, 22(6), 435–455. doi:10.1111/j.1365-2575.2011.00393.x

Wilcocks, L. (2013). *Information management: the evaluation of information systems investments*. Springer Science Business Media.

Winniford, C. (2009). *Confusion in the Ranks: IT Service Management Practice and Terminology*. Academic Press.

Wui-Gee, A. (2009). *Implementing IT service management: A case study focussing on critical success factors*. Stillwater: International Association for Computer Information Systems.

Yin, R. (2014). *Case Study Research, Design and Methods* (5th ed.). SAGE Publications.

Yusuf, Y., Sarhadi, M., & Gunasekaran, A. (1999). Agile manufacturing: The drivers, concepts and attributes. *International Journal of Production Economics*, 62(1-2), 33–43. doi:10.1016/S0925-5273(98)00219-9

Zhang, Z., & Sharifi, H. (1999). A methodology for achieving agility in manufacturing organizations: An introduction. *International Journal of Production Economics*, 62(1-2), 7–22. doi:10.1016/S0925-5273(98)00217-5

Zheng, Y., Venters, W., & Cornford, T. (2011). Collective agility, paradox and organizational Improvisation: The development of a particle physics grid. *Information Systems Journal*, 21(4), 303–333. doi:10.1111/j.1365-2575.2010.00360.x

Zhong, X. (2010). An ITIL based ITSM practice: A case study of steel manufacturing enterprise. *7th International Conference on Service Systems and Service Management*.

KEY TERMS AND DEFINITIONS

Data Collection: It is the process of gathering data from a variety of relevant sources in an established systematic fashion for analysis purposes.

Incident: An observable change to the normal behavior of a system.

Incident Management: The activities of an organization to identify, analyze, and correct organizational hazards.

ITAM: IT asset management (ITAM) is a type of business management directly linked to the company's IT infrastructure. With ITAM, professionals review an organization's complete hardware and software inventory and make complete decisions on procurement, usage and all other aspects related to an asset's life cycle.

ITSM: IT service management (ITSM) describes a strategic approach to designing, delivering, managing and improving the way information technology (IT) is used in the enterprise. The goal of any IT service management structure is to ensure that the right processes, people and technology are in place so that the business can achieve its business objectives.

Maturity: A measurement of the ability of an organization to undertake continuous improvement in a particular discipline.

Maturity Model: A set of structured levels that describe how well an organization can reliably and sustainably produce required outcomes.

Use-Case: It is a list of events and actions among systems and users in a specific environment and for a specific goal.

APPENDIX

Table 12. ITSM/ITAM maturity assessment interview (sample)

IT Service Management		Answer
Self-Service Desk	Is there a service center in your organization (formal or informal)?	Yes we do it every few years
	Are calls that are taken at the Service Desk recorded in an electronic system?	Yes at least half of them are/do
	Does the service center log incoming calls and emails in a helpdesk system?	Yes we do it every few years
Incident Management	Does IT staff have a clear understanding of the incident management process?	Yes at least half of them are/do
	Is there enough information recorded incidents when they are registered?	Yes we did it once
	Is there a classification code assigned to incidents that can indicate the probable cause of the incident?	Yes at least half of them are/do
Problem Management	Does IT staff have a clear understanding of the problem management process?	Yes we do it every few years
	Is it clear to whom in the organization should the problems be attributed?	Yes at least half of them are/do
	Are the time and budget allocated to staff training in this area sufficient?	Yes at least half of them are/do
	Does the process owner analyze incident information to identify trends in incidents?	Yes a small percentage are/do
Release Management	Is there sufficient time and budget allowed for training staff in this process area?	Yes at least half of them are/do
	Is there a published and accepted list of what is considered to be the highest priority components of the infrastructure?	Yes a small percentage are/do
	Is there a known and documented naming convention for all configuration elements (CIs)?	Yes at least half of them are/do
	Is there a well-defined release management process within the organization?	Yes a small percentage are/do
Change Management	Does IT staff have a clear understanding of the change management process?	Yes we do it every few years
	Are change requests checked and verified prior to submission?	Yes at least half of them are/do
	Is there sufficient time and budget allowed for training staff in this process area?	Yes we do it every few years
	The Advisory Council on Change (ACC) establishes an appropriate mandate (meeting time, authority, etc.)?	Yes at least half of them are/do

continued on following page

IT Management Agility in Large Organizations

Table 12. Continued

Service Level Management	Does IT staff have a clear understanding of the SLA management process?	Yes teams write/run their own
	Is there a regular review of the activities associated with this process?	Yes we do it every few years
	Are there Service Level Agreements (SLAs) that follow a defined structure?	Yes we do it every few years
	Does this process area exchange information with a variety of other process areas?	Yes we do it every few years
Availability Management	Are there regular reviews of the performance of this process area against documented Key Performance Indicators (KPIs) on a regular basis?	Yes at least half of them are/do
	Are the availability objectives set by the organization SMART (Simple, Measurable, Achievable, Realistic, Time-bound)?	Yes a small percentage are/do
	Are electronic tools used in this process field well utilized?	Yes at least half of them are/do
Capacity Management	Alarm thresholds are in place for systems that alert personnel to approaching maximum capacity limits?	Yes at least half of them are/do
	Are the differences between operational capability, service capability and resource management well defined?	Yes a small percentage are/do
	Does this process area exchange information with a variety of other process areas?	Yes a small percentage are/do
IT Asset Management		Answer
Asset Discovery and inventory	Is there a defined procedure for managing the organization's information assets?	Yes a small percentage are/do
	Which tool do you currently use to discover your software and hardware assets?	Yes but on an ad-hoc basis
Configuration Management	Is there a published and accepted list of what are considered to be the most critical components of the infrastructure?	Yes there is a standard set
	Is there a known and documented naming convention in place for all Configuration items (CIs)?	Yes, a small percentage are/do
	Are there procedures to ensure that the configuration management process cannot be bypassed?	Yes there is a standard set
IT Financial Management	Do you have an effective control over the operating costs of the IT environment?	Yes, a small percentage are/do
	Can costs of providing current services to the business be demonstrated easily?	Yes, localized to business areas
	Are actual costs compared to budgeted costs on a regular basis?	No

continued on following page

Table 12. Continued

Asset Lifecycle	Has the organization implemented, or plan to implement an asset management system?	Yes on an ad-hoc basis
	Does the organization have an asset management inventory/database, or does it plan to develop one?	No
IT Security Management		Answer
IT Service Security Management	Is there a procedure for IT services security management?	Yes we do it every few years
	Are there any security applications implemented in the organization?	Yes at least half of them are/do
IT Asset Security Management	Are the company's security requirements well documented?	Yes at least half of them are/do
	Is there a clear understanding of who or which department is responsible for IT security?	Yes at least half of them are/do
	Are there physical barriers in place preventing unauthorized access to critical IT equipment?	Yes a small percentage are/do
Vulnerability and Risk Management	Is there an automated risk management process conforms to international standards?	Yes at least half of them are/do
	The organization defines the system criticality according to its risk?	Yes a small percentage are/do
Compliance Management	Is there a formal policy containing, or referring to all security requirements to ensure compliance with the organization's security standards?	Yes a small percentage are/do
Agility Management		Answer
Strategy and Process	Does IT staff have a clear understanding of the agility management process?	Yes on an ad-hoc basis
	Is there a regular review of the activities associated with this process?	Yes a small percentage are/do
Flexibility of Structure	The organization has qualified and motivated people at its disposal, enabling it to provide agile solutions for changing the business situation?	No
	The organization provides processes, plans, and responsibilities for agile responses to a changing business environment?	Yes on an ad-hoc basis
Up-to-Dateness of Technology Systems	Are IT services provided in accordance with business needs ?	Yes teams write/run their own
	Do the organization's IT-focused programs deliver benefits in a timely manner and meet quality requirements and standards?	Yes a small percentage are/do
	Does IT service center provide knowledge, expertise, and initiatives for business innovation?	No
	Are the benefits derived from IT investments and the IT services portfolio?	No

continued on following page

IT Management Agility in Large Organizations

Table 12. Continued

Staff competency and skills	Does the organization cultivate its expertise through effective training?	Yes at least half of them are/do
	Does the organization motivate and maintain proficient employees?	Yes a small percentage are/do
	Are IT staff encouraged to improve their technical skills and are trained in development methods and tools to support agile development technics?	Yes a small percentage are/do
Organizational Agility	Are IT resources optimized to meet the organization's agility objectives?	No
	Does the organization provide effective business processes?	Yes on an ad-hoc basis
	Does the organization define, maintain and approve functional requirements after a quick analysis of feasibility and alternate solutions?	No

Chapter 6

Managing the Cloud for Information System Agility in Organizations

ABSTRACT

In 2007, cloud computing was introduced to the IT dictionary. The theme is attracting growing interest from both the IT world and the business players who need to enhance information systems agility, reduced costs, or reduce dependence on internal IT teams when they are judged too slow. However, the fact that cloud computing, as presented by providers, increases the agility is unclear. Business managers, IT professional, and academics are querying the relationship between cloud computing and IT agility. This chapter aims to understand cloud computing's role in improving IT agility by introducing recent studies in the IS and IT management literature. This chapter argues that cloud computing impact IS performance by organizational capabilities (agility). The authors also propose a conceptual framework to improve IS agility by cloud computing based on DevOps. One of the primary motivations of this research is the lack of fieldwork when considering how cloud computing improves information systems agility.

DOI: 10.4018/978-1-5225-7826-0.ch006

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Since 2007, the year that the two leaders in cloud computing IBM and Google have invested in the construction of large data centers that can be used by students over the Internet to remotely program and research, known as cloud computing (Lohr, 2007). The cloud infrastructure was also recognized as a cost-effective model for delivering information services, reducing IT management complexity, promoting innovation and improving real-time responsiveness. For many organizations (Buxmann, Diefenbach, & Hess, 2015) and countries (Changchit & Chuchuen, 2018), cloud infrastructure has served as a platform for developing innovation and a highly qualified human resource capacity. In 2011, the US federal government estimated that 20 billion dollars of the IT investment budget, which is 80 billion dollars, would be a potential target for cloud computing solutions migration (Metheny, 2013).

Cloud Computing has had a major impact on information technology (IT) during recent decades as leading companies such as Google, Amazon and Microsoft have focused on providing more efficient, secure and cost-effective cloud platforms for organizations that are trying to redefine their business models using the concept. Cloud Computing is one of the major technologies that has revolutionized the world of computing. The IT service delivery model provides significant benefits. This enables today's organizations to adapt proactively their IT infrastructure to faced rapidly changing environment and business requirements. Importantly, it significantly reduces the complexity of IT management, enabling more use of IT. Cloud-based services offer also interesting reuse opportunities and design challenges for application developers and platform providers. Cloud Computing has therefore generated a lot of enthusiasm among technologists and researchers in general.

For many organizations, cloud computing can be a driving factor of change, enabling them to make optimal use of information and communication technologies without investing massively at the outset and avoiding the risks of getting stuck with obsolete technologies. With cloud computing, providers can provide an information and communication technology infrastructure as a service to end customers (Fernando, Loke, & Rahayu, 2013; K. H. Kim, Beloglazov, & Buyya, 2009). By using cloud computing, organizations can reduce the cost of information and communications technology acquisition and maintenance, attracting new customers, increasing revenue, preserving profitability, and improving agility (Goyal & Dadizadeh, 2009; Sean

Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011). Companies that have made lower investments in information and communications technology infrastructure are more apt to adopt and use cloud computing (Bhat, 2013). Large enterprises are increasingly adopting cloud computing (Gupta et al., 2013; Li et al., 2011).

In 2017, the situation changed radically. Forty-eight companies of the fifteen “Fortune Global 50” (Brinda & Heric, 2017) companies have publicly announced their cloud adoption plans. Today, cloud computing is increasingly becoming the leading technology to do business for the next generation. The agility of the cloud enables enterprises accelerate time to the marketplace by reaching various parts of the development chain. Due to promises of information technology (IT) efficiency and business agility, they are integrating cloud computing into their IT strategies (John, Morrison, & Fox, 2018). Cloud computing is a combination of two key IT tendencies: IT efficiency, where IT performance is used more efficiently, and business agility, where information technology is a competitive tool through rapid deployment, batch parallelism and business intensive analytics (Avram, 2014).

Cloud computing infrastructures can improve the efficiency with which companies can use their investments in information technologies through the unification of separate systems and automation of the management of the group of systems as a unified entity. A cloud infrastructure can be a cost-effective model for delivering information services, reducing IT management complexity, promoting innovation and increasing responsiveness through real-time.

Many customers are interested in cloud infrastructure as a platform for innovation, particularly in countries that want to foster the development of a highly skilled and high-tech workforce. Reduce operating costs: The resources of a cloud environment can be rapidly assigned and unallocated according to demands. Therefore, a service provider can achieve significant operating cost savings through resource liberation when service demand is low. Cloud Computing is a combination of two trends in information technology, IT efficiency and commercial agility, through information technologies, which provide a competitive factor through rapid and parallel deployment, batch processing, etc.

It is noted that the number of organizations adopting cloud computing continues to increase (Smith, 2017). The purpose of this chapter is to provide recommendations for decision-makers in information technology and to explain the cloud computing technology in agility terms. Cloud computing is a growing technology and its strengths and weaknesses have not yet been

fully studied, documented and tested. This chapter proposes recommendations on when and how cloud computing is an effective tool, and outlines the limitations of recent studies and the perspectives for future research.

Problem Statement

Cloud Computing is a new model to meet the IT needs of businesses. Based on service, flexibility, and cost-effectiveness. One of the important benefits of cloud computing is the agility it brings to an organization's IT and, therefore, to the organization itself. Most research cites agility as one of the major attributes of cloud computing (Phan et al., 2012) and it is considered that cloud computing improves information system (IS) agility. However, it is not clear how cloud computing, once integrated into an organization's existing IS, increases the agility of the entire IS, and how assessed the claimed improvement agility.

Although enterprise adoption of cloud computing is increasing, cloud computing has not yet reached maturity, and little research has been conducted to determine the impact of cloud computing on the agility of information systems (Yang, Huff, & Tate, 2013). Decisions makers require to achieve the agility improvements obtained by deploying cloud computing. This capability allows them to understand the state of change both before and after its implementation and make an appropriate decision about adopting cloud computing into their investment portfolios.

Goals and Objectives of the Research Study

This research focuses on factors related to the cloud computing adoption process, and in particular the impact of agility on how to integrate cloud-computing technology into information systems. It mainly aims to explore how agility changing influences decision-making and how cloud computing will increase agility of information systems. The research question addressed is how adopting cloud computing improve IS agility?

Previous research, Yang et al. (2013) provides preliminary empirical evidence that agility and one of the factors influencing decision-making concern the adoption of cloud computing technology as well as its role in increasing the agility of information systems. Our study builds on these studies by theorizing and empirically validating the factors influencing the decision to adopt cloud- computing technology.

The two research questions of interest to this study are:

- What factors, drive this cloud computing technology and why?
- To what extent are cloud-computing adoption improve information systems agility?

To address these questions, we draw the technology acceptance model (TAM) and prior Diffusion of innovation (DOI) research to propose a cloud adoption model and framework to improve IS agility through cloud technology.

The chapter proceeds as follows. The following section looks at the literature on factors influencing cloud computing adoption deaths in order to construct a theoretical model for cloud technology adoption. The second section describes empirical studies that test the proposed model. The third section describes the construction and validation of a framework to increase IS agility through cloud computing this framework is the subject of a qualitative study. The last section presents the research finding and discussion.

BACKGROUND AND LITERATURE REVIEW

This literature review synthesized current cloud research from the perspective of organizations. It integrates results using an established framework; our results are structuring according to the following four aspects: cloud-computing properties, adoption characteristics, governance process, and impact on the information system agility. This section highlights a shift in focus from technology issues to a broader understanding of cloud computing as a new information technology concept. There is a growing recognition of its characteristics and fundamentals of the concept. However, research on the factors that drive or limit cloud adoption of services, as well as empirical research on agility through the cloud, is rare. This can be due to that cloud computing is a recent and relatively new research topic (Adamson, Wang, Holm, & Moore, 2017). Research on the different phases of service cloud deployment is also at a developmental stage.

Although this concept is not completely new, there is no universal or standard definition of cloud computing (Foster, Zhao, Raicu, & Lu, 2008; Gong, Liu, Zhang, Chen, & Gong, 2010; Sultan, 2010). It has evolved with recent advances in virtualization technology, cloud computing and Internet-based service delivery. The “cloud” metaphor refers to the ubiquitous availability and accessibility of computer resources through Internet technologies (Sultan,

2010; Vouk, 2008). With cloud solutions, enterprises and consumers can easily access large amounts of computing performance at negligible cost (W.-W. Wu, Lan, & Lee, 2011). Transferring IT capabilities such as storage, applications and services towards the cloud offers companies the ability to potentially reduce the cost of overall information technology (Goscinski & Brock, 2010; Martens & Teuteberg, 2012; Stanoevska, Wozniak, & Ristol, 2009). Cloud computing thus offers monetary advantages organizations could certainly not ignore.

Typically, there are three types of cloud computing services (Chang, De Roure, Wills, & Walters, 2011). In Infrastructure as a Service (IaaS), the computing and storage power base units are cloud-based and available on demand (for example, Amazon Elastic Compute Cloud (EC2), Rackspace, Amazon Simple Storage Service (S3), and GoGrid). Among the advantages of this model are pay-for-use and resource elasticity to satisfy computation needs (Thomas, Redmond, & Weistroffer, 2009). In the case of Platform as a Service (PaaS), the service provider offers a stack of integrated solutions to create and deploy applications from the cloud (e.g. Salesforce, Google AppEngine and Microsoft Azure). This model has the advantage of being able to provide all the elements of software development (design, testing, version control, maintenance and hosting) via the Internet (Stanoevska et al., 2009). SaaS (“Software as a Service”) is essentially the ability to access cloud-based applications using a thin client (such on a web browser or mobile application) instead installing software to their own computer (e.g. Joyent and Salesforce CRM). Among its advantages are centralized configuration and hosting, updates to current software versions without the need for reinstallation, and accelerated feature delivery (Dillon, Wu, & Chang, 2010).

Cloud computing represents the intersection of IT effectiveness and business agility (Kim, 2009). IT performance results from the use of scalable hardware and software resources (Marston, Bandyopadhyay, & Ghalsasi, 2011), improved work efficiency and coordination between firms (Abdollahzadehgan, Che Hussin, Gohary, & Amini, 2013), and highly available services (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, et al., 2010). The business agility of cloud computing is the ability to rapidly deploy computing tools, reduce initial capital expenditures (Hoberg, Wollersheim, & Krcmar, 2012; A. Lin & Chen, 2012), and respond quickly to changing market needs (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, & Rabkin, 2010; Hoberg et al., 2012). Cloud Computing removes traditional boundaries between enterprises. This ability to seamlessly, deliver IT functions as cloud-based solutions have proven to be viable and

cost-effective, as demonstrated by its growing adoption. Li, Zhang, O'Brien, Cai, and Flint (2013) aimed at evaluating and comparing commercial cloud services, compiled a de facto metrics catalog using a systematic literature review (SLR) of current cloud services assessment work. Yang et al. (2013) looked at conceptualizing IS agility based on previous research to assess the contribution of different cloud computing services to IS agility.

From the reduced complexity and unlimited scalability to the on-demand capacity and cost savings of CapEx, Cloud Computing delivers all the promise. While there are still many unanswered questions about cloud computing, many companies are optimistic about their ability to deliver on these promises. Regardless of how well cloud-computing delivers on its promise, one thing is certain: organizations are not willing to sacrifice security, visibility and control to move to the cloud. They need to know what is happening in the cloud, how their applications are delivered and how traffic is controlled and directed. A must-have in cloud computing is agility: the capacity that enables enterprises to respond rapidly and accurately to unexpected and changing business demands. Agile enterprises, those that can provide on-demand IT services under all workload conditions, can seize new opportunities and remain competitive. This fact prompted us to continue this research in order to verify whether cloud computing is able of improving IT agility. Table 1 summarizes our literature review, highlighting the different methodologies and contributions.

CLOUD COMPUTING ADOPTION MODELS

Technology-Organization-Environment (TOE) Framework

Tornatzky, Fleischer, and Chakrabarti (1990) outlines the TOE framework in order to understand the innovation process in an enterprise context. It addresses three factors that influence adoption of innovation: technology, organization and the environment. Technology context means the internal and external technologies pertinent to the organization and those that could be adopted. Organizational context relates to company descriptive characteristics (i.e. size, organizational structure, level of centralization), resources (human and insufficient resources) and communication process (formal and informal) among employees. With respect to the environment, this context includes environmental market elements, competitors and the regulatory framework

(Oliveira & Martins, 2011; Oliveira & Martins, 2010; Tornatzky et al., 1990; Zhu & Kraemer, 2005).

Several research studies have examined technical and operational issues related to cloud computing, involving topics such as selecting cloud computing services in terms of cost and risk (Martens & Teuteberg, 2012), secure storage audit protocol and computing in the cloud. cost of cloud computing ownership models (Mazhelis & Tyrväinen, 2012; Tan & Ai, 2011; Walterbusch, Martens, & Teuteberg, 2013), and security issues, privacy risks and information loss (A. Y.-L. Chong, Ooi, Lin, & Raman, 2009; Wang, 2010). Our search of scholarly databases found only a few published journal articles that addressing cloud computing adoption from an organizational perspective as shown in Table 1. (Abdollahzadehgan et al., 2013) used the DOI and TOE framework to study the adoption of cloud computing in Taiwan's high-tech industry. Their research model was not expansive because it did not address key factors such as cost savings and security concerns that are critical to the enterprise's adoption of cloud computing. They also assessed cloud adoption as a dynamic dependent variable rather than a continuous process. Lin and Chen (2012) interviewed 19 IT professionals in Taiwan using a semi-structured interview format. According to their qualitative assessment, IT organizations are hesitant to adopt cloud computing until the uncertainties associated with cloud computing (e.g., security and standardization) are further resolved and effective business models emerge. Trigueros-Preciado, Pérez-González, and Solana-González (2013) used a qualitative and quantitative analysis methodology to identify barriers to cloud adoption. They surveyed 94 Spanish SMEs and concluded that knowledge of cloud computing was low among companies and that companies knew nothing about cloud computing.

Our search of scholarly databases found only a few published journal articles that assess cloud-computing adoption from an organizational perspective as shown in Table 1. Abdollahzadehgan et al. (2013) used the DOI and TOE framework to study the adoption of cloud computing in Taiwan's high-tech industry. Their research model was not expansive because it did not address key factors such as cost savings and security concerns that are critical to the enterprise's adoption of cloud computing. They also assessed cloud adoption as a dynamic dependent variable rather than a continuous process. Lin and Chen (2012) interviewed 19 IT professionals in Taiwan using a semi-structured interview format. According to their qualitative assessment, IT organizations are hesitant to adopt cloud computing until the uncertainties associated with cloud computing (e.g., security and standardization) are further resolved and effective business models emerge.

Trigueros-Preciado et al. (2013) used a qualitative and quantitative analysis methodology to identify barriers to cloud adoption. They surveyed 94 Spanish SMEs and concluded that knowledge of cloud computing was low among companies and that companies knew nothing about cloud computing adoption. Nkhoma, Dang, and De Souza-Daw (2013) used secondary data from the survey of a large services company to study the drivers and barriers to cloud computing adoption. Wu, Cegielski, Hazen, and Hall (2013) investigated whether the information processing requirements and capacity affect the firm's intention to adopt cloud computing; they used the DOI theory and information processing view (IPV) to conduct their study in the supply chain domain.

Abdollahzadehgan et al. (2013) proposed using the TOE framework to evaluate the barriers to cloud computing adoption in SMEs; their study did not include hypothesis testing or empirical validation. Kshetri (2013) used the institutional theory to investigate the perception and security issues based on the context provided by formal and informal institutions; no empirical assessment was provided. The review of published journal articles indicates that most studies empirically evaluate the direct effects of innovation, contextual factors or conduct analysis using qualitative methods or secondary data on the adoption of cloud computing. No study has taken a holistic approach to empirically validate the direct and indirect effects of the innovation characteristics and the underlying technology, organization, and environmental contexts. Yang and Tate (2012) voice similar concerns by classifying the published journal articles on cloud computing into four research themes: technological, business issues, domains and applications, and conceptualization.

Based on a descriptive literature review of 205 refereed journal articles, their study indicates that research on cloud computing is skewed mostly toward technological issues. They highlight the paucity of cumulative research to address the social, organizational, and environmental perspectives of cloud computing. This study addresses this crucial research gap by developing an integrative research model that combines the theoretical perspectives of the diffusion of innovation and the technology, organization, and environmental contexts.

Combining DOI and TOE

To determine the concepts of the integrative search model, an extensive search was conducted using the DOI and TOE framework, including EBSCO

Table 1. Cloud computing studies

Author	IT adoption (dependent variable)	Constructs/factors (independent variables)	Methods	Data and context
(Abdollahzadehgan et al., 2013)	Cloud computing	Technology (relative advantage, complexity, compatibility), Organization (top management support, firm size, technology readiness) and Environment (competitive pressure, trading partner pressure)	Conceptual	Conceptual Model
(Low, Wu, & Chen, 2011)	Cloud computing	Technology (relative advantage, complexity, compatibility),	Factor analysis (FA), logistic regression	E-mail survey of 111 firms belonging to the high tech
(Y. Wu et al., 2013)	Cloud computing	Business process complexity, entrepreneurial culture, compatibility, application functionality	Confirmatory factor analysis, multiple regression analysis	E-mail survey of N=289 firms in Manufacturing and retail
(Nkhoma & Dang, 2013)	Intention to adopt cloud computing	Adopter's style as moderator of perceived technology barriers, perceived environmental barriers, perceived benefits	Partial least squares (PLS)	Using secondary data
(A. Lin & Chen, 2012)	Cloud computing	Relative advantage, compatibility, complexity, Trial-ability, observability	Semi-structured Qualitative interview	19 IT professionals, Taiwan
(Trigueros-Preciado et al., 2013)	Cloud adoption	Barriers and benefits	Qualitative and quantitative methodology	Survey N=94 SMEs in Spain
(N Kshetri, 2016)	–	Regulative, normative, cognitive	Conceptual	Survey of Cloud Vendors in China N=7

Academic Search, all ProQuest databases (e.g. ABI/INFORM Global), PsycNet databases, and Springer, Science Direct and Google scholar. Subsequently, the well-cited studies have been consolidated to identify the most representative factors evaluated in the published literature on adoption studies. Finally, we also examined each construction to identify its applicability in adopting cloud computing. The factors identified by this systematic approach and the dependent variable measured by them are summarized in Table 2.

Many research calls for an approach that combines more than one theoretical perspective to understand the adoption of new innovative technologies by information systems (Fichman, 2004; Oliveira & Martins, 2011; Wu et al., 2013). As such, to better comprehend the organizational decisions that relate to the adoption of technological innovation, the study context must be global

and the variables adapted to the specificity of the innovation (Adams et al., 2009). (DOI) and (TOE) methods are widely used in many IT adoption studies and had received ongoing empirical support. Also, The value of context integration (TOE) to reinforce DOI theory is recognized (Lin & Lin, 2008; Oliveira & Martins, 2011; Wu et al., 2013). Implicitly, the technological context is the same idea as (Rogers, 2003). The DOI has the same internal and external organizational characteristics as the TDE organizational context (Hsu, Kraemer, & Dunkle, 2006). There are also important differences between the two theories. The TOE does not specify the role of individual characteristics (e.g., senior management support). At this point, DOI suggests that executive support is included in the context of the organization. Likewise, the DOI ignores the impact of the environmental context. As a result of the limitations of DOI, TOE provides more insight into IT adoption by including technology, organizational and environmental contexts (Zhu, Dong, Xu, & Kraemer, 2006). Consequently, the two theories significantly complement each other (Oliveira & Martins, 2011).

Of the five DOI attributes, there are three innovation characteristics applicable to cloud adoption: relative advantage, complexity, and compatibility. Experimentation and observational capacity are not widely used in IT innovation studies (A. Y.-L. Chong et al., 2009). Thus, by following general information, systems research guidelines; we ignore these two attributes because they are not relevant to cloud computing technology. Rogers (2003) states that “the nature of the innovation determines the type of relative benefit that is important to the adopter” and that the relative benefit of the innovation can be “expressed in terms of economic profitability, social prestige or by other means. In our study, we postulate that cloud computing can lead to an economic advantage in terms of cost reduction (Ifinedo, 2011) that it is capable of improving IS agility (Yang et al., 2013). Similarly, security concerns can reduce the relative benefits of cloud computing. We, therefore, include two additional attributes, namely cost savings, and security as antecedents to the relative advantage of cloud computing. They determine whether cloud computing can be relatively beneficial in achieving cost savings, improving IT agility to meet change, seize new opportunities and remain competitive.

RESEARCH MODEL AND HYPOTHESES

From the TOE framework, the technology context determines whether the technological readiness of the firm will constrain or facilitate the adoption

Table 2. Summary of the factors studied influencing cloud adoption

Sources	Model / Theory	Factors												
		Agility	Security Issue	Cost-Saving	Top Management Support	Competitive	Firm Size	Technological	Regulatory Support	Competitive Pressure	Compatibility	Complexity		
(A. Lin & Chen, 2012)	DOI	*										*		*
(Y. Wu et al., 2013)	DOI & Others											*		*
(Abdollahzadehgan et al., 2013)	TOE				*	*	*	*			*	*		*
(Low, Wu, & Chen, 2011)	DOI & TOE		*	*					*		*	*		*
(Nkhoma & Dang, 2013)	TOE					*			*					
(K. Zhu, Kraemer, & Xu, 2006)	TOE		*				*			*				
(K. Zhu, Dong, et al., 2006)	TOE & Others		*	*			*				*	*		*
(K. Zhu & Kraemer, 2005)	TOE							*	*	*	*			
(H.-F. Lin & Lin, 2008)	TOE								*	*	*	*		*
(Kuan & Chau, 2001)	TOE			*	*		*		*	*	*	*	*	*

continued on following page

Table 2. Continued

Sources	Model / Theory	Factors												
		Agility	Security Issue	Cost-Saving	Top Management Support	Competitive	Firm Size	Technological	Regulatory Support	Competitive Pressure	Compatibility	Complexity		
(Ringle, Sinkovics, & Henseler, 2009)	TOE				*		*				*		*	*
(Ghobakhloo, Arias-Aranda, & Benitez-Amado, 2011)	TOE			*	*		*	*				*		
(Klein, 2012)	TOE				*		*					*		*
(Tsai, Lee, & Wu, 2010)	DOI			*	*		*				*			
(A. Y.-L. Chong et al., 2009)	DOI										*			*
(Azadegan & Teich, 2010)	DOI & TOE						*				*			*
(Alam, 2009)	DOI & TOE				*		*				*			*
(Adams et al., 2009)	DOI & TOE			*	*						*			
(Yang et al., 2013)	-	*						*						*
(Rimienė, 2011)	-	*						*						
(Siegel & Perdue, 2012)	-	*	*										*	*

of cloud computing. Factors specific to the organization context are top management support and firm size. The extent to which the environmental context may influence the firm's decision to adopt cloud computing is identified by two variables, competitive pressure and regulatory support. The integrative research model is illustrated in Figure 1. By associating the innovation characteristics of cloud computing with the technological, organizational and environmental contexts of the TOE framework, we are acting on researchers' call to build a more holistic model to understand the diffusion of IT innovation (Kalle & M., 2003; Oliveira & Martins, 2011; Y. Wu et al., 2013).

Hypotheses of Innovation Characteristics

Agility

The most important advantage of Cloud computing is that it adds to the agility of an organization. With the use of cloud computing, enterprise systems are being transformed, allowing organizations greater flexibility in the use of services, greater flexibility, and greater productivity (Kunio, 2010). According to Sitaram and Manjunath (2012), agility and innovation are considered the main growth drivers offered by cloud computing. Companies willing to reconfigure around cloud computing would be more adaptable to changing external markets and better positioned to exploit new opportunities by leveraging the scalability and agility of cloud computing (Altaf & Schuff, 2010; Weinhardt et al., 2009).

Thus, **H9**. Agility can positively influence the relative benefits of cloud computing.

Cost-Savings

Cloud computing technology offers opportunities for innovation, reduces IT spending and reduces the total cost of computing (Cervone, 2010). By allowing companies to focus on their core business rather than being stifled by technological change, cloud computing fosters innovation. By choosing cloud computing, an enterprise can reduce the time spent on system maintenance and the time required for routine upgrades. Cloud computing also reduces infrastructure costs, reduces energy consumption and reduces maintenance costs (Mazhelis & Tyrväinen, 2012). Thanks to vendor specialization, cloud

computing service providers can offer IT functions at lower cost and deliver economies of scale to the end user (Benlian & Hess, 2011). As a catalyst for the rapid adoption of changing technologies, the cloud offers cost-effective ways to transform businesses by reinventing an organization's way goods and services are sold and used.

Hence **H1b**. Cost-savings would positively influence the relative benefits of cloud computing.

Security Issue

The term security breach refers to an incident in which a company or government organization loses sensitive information, personal data or other confidential information (Bishop, 2002). Cloud computing is a convergence of storage and computing in a multi-user shared environment. Which increases security risks (Schneiderman, 2011; Shen & Tong, 2010), due to the fact that organizations are not aware of and uncertain about potential security risks (Benlian & Hess, 2011). In addition, the lack of mature security protocols and identity management standards means that organizations will be reluctant to adopt a cloud computing solution. Migration to the cloud adds new layers of complexity to data security, which significantly influences the company's decision to adopt an innovation.

Hence; **H1a**. The security and privacy issues will have a negative impact in terms of cloud computing's relative advantage.

Relative Advantage

Relative advantage is defined as the measure to which an innovation is considered more beneficial than the idea replaced (Rogers, 2003). Innovations with a clear and unequivocal advantage in strategic effectiveness (e.g., improved revenues) and operational efficiency (e.g., cost savings) have a stronger incentive to adopt (Trisha, Glenn, Fraser, PAUL, & Olivia, 2004) In the case where the advantages of technology (in this case cloud computing) outweigh existing processes and practices (Ifinedo, 2011), the benefits will impact positively on its adoption.

Therefore, **H1**. The relative advantage will have a positive influence on cloud computing adoption.

Complexity

Complexity is the stage where an innovation is considered relatively difficult to comprehend and use (Ivancic, 2003). The easier the technology is to integrate into business operations, the greater the likelihood of its adoption. Cloud environments provide the ability to instantly pool resources to meet workloads. However, moving to a cloud solution can be a challenge for organizations that lack technical expertise and IT specialists. For example, integrating existing applications with a specialized cloud infrastructure (for example, Oracle's Elastic Cloud or HP's Cloud System) may require a level of expertise which is not available easily within the enterprise. Also, the use of cloud-based solutions presents challenges when defined limits for securing business processes and data privacy in a multi-tenant, shared environment are not fully refined (Crook & Kumar, 1998).

Hence, **H2**. Complexity will have a negative influence on cloud adoption.

Compatibility

Compatibility is the degree to which the innovation corresponds to the existing values, past practices and current needs of the potential adopters (Ivancic, 2003). Compatibility is an important determinant of innovation adoption (Sila, 2010; Azadegan & Teich, 2010; S. Chong & Bauer, 2000; Dedrick & West, 2004). For example, if the purpose of cloud adoption is to take advantage of the scalability benefits of low-security applications, transferring capacity to cloud infrastructure makes economic sense. For example, business capacity and operability are factors that will determine whether cloud computing should be adopted by an organization.

So, **H3**. The Compatibility can Positively Affect Cloud Adoption.

Technological Readiness

The technology context refers to the technological characteristics available in the organization for the adoption of technology. It includes both the structural aspects and the specialized human resources. The structural aspects refer to the platform or the technological infrastructure (e.g., installed network technologies and enterprise systems) within the firm that the cloud-computing services can complement or replace (e.g., implementing a collaborative document sharing solution using cloud-based storage). The specialized human

resources are the people within the organization who have the knowledge and skill to implement the cloud-computing services (e.g., employees with computer skills, IT specialists) (Lim, 2009). Together they enhance the technological readiness of an organization. Therefore, firms with a higher degree of technological readiness are better positioned for the adoption of cloud computing.

Hence, **H4**. Technological readiness will positively influence cloud-computing adoption.

The Organization Context

Top Management Support

Organizational context refers to the availability of resources that support the adoption of an innovation (Lippert & Govindrajulu, 2006); that is, organizational characteristics which facilitate or limit a firm's adoption and implementation of the innovation. Many factors affect the relationship with the organizational structure and innovation adoption, such as the level of centralization, distribution of power and control, information linkages, availability of insufficient resources, lateral communication, firm size, and senior management support (Tornatzky et al., 1990; Xu & Quaddus, 2012). Among these, senior management support and enterprise size are the most important factors in assessing cloud adoption (Lippert & Govindrajulu, 2006). Senior management support plays an important role in the adoption of IT in the cloud by supporting the decision to allocate the necessary resources, integrate services and re-engineer processes (Abdollahzadehgan et al., 2013). When senior management fails to recognize the benefits of cloud computing to the business, one must wait for the opposition to adoption.

So, **H5**. Top management support will have a positive influence on cloud adoption.

Firm Size

Another organizational factor can influence cloud adoption. Indeed, large firms have an advantage over small firms because they have more resources and are able to take more risks associated with adopting the innovation (Thiesse, Staake, Schmitt, & Fleisch, 2011; Zhu, Kraemer, et al., 2006). Research has shown that small firms while more versatile, do not easily adopt new

technologies (Lippert & Govindrajulu, 2006). As a result, enterprise size is a determining factor in the adoption of cloud computing (Abdollahzadehgan et al., 2013).

Hence **H6**. Firm size will have a positive influence on cloud adoption.

The Environment Context

The Competitive Pressure

The environmental context is the framework in which a company operates and depends on the nature of the industry, its competitors, its ability to access resources provided by others and government relations (Lippert & Govindrajulu, 2006). Among these, the drivers that have an impact on cloud adoption are business competition and the regulatory environment (Zhu, Kraemer, & Xu, 2003). In the literature on the diffusion of innovation, competitive pressure has long been seen as an important driver for technology diffusion. It refers to the pressure exerted by competitors in the industry (Abdollahzadehgan et al., 2013; Zhu et al., 2003). Adopting new technologies is often a strategic necessity to compete in the marketplace. Cloud Computing enables enterprises to benefit from greater operational efficiency, better market visibility and more accurate access to real-time data (Misra & Mondal, 2011).

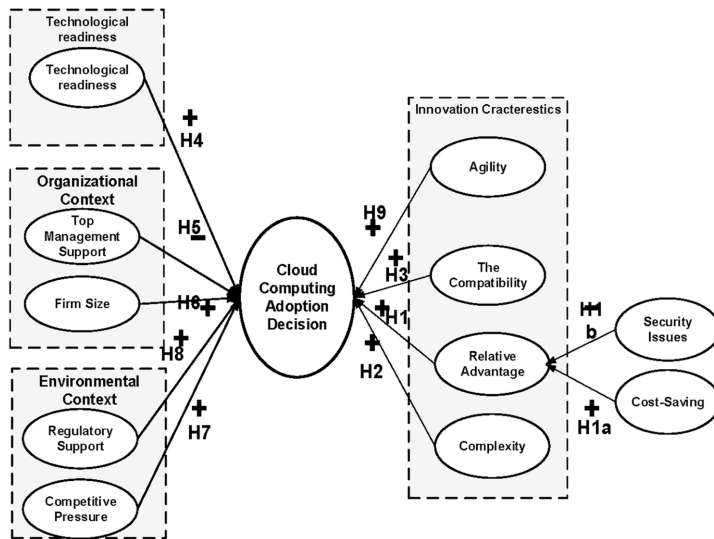
That is why **H7**. The competitive pressure will influence the adoption of cloud computing positively.

Regulatory

Regulatory support is defined as the support provided by a government authority to encourage companies to assimilate computer innovation (Zhu, Kraemer, et al., 2006). The impact of existing laws and regulations can be crucial for the adoption of new technologies. Government regulation can encourage or discourage companies from adopting cloud computing. For example, legislators in the United States and European Union member states have specific mandates to protect organizational data. When a government requires enterprises to comply with cloud-specific standards and protocols, enterprises will be more inclined to adopt cloud computing.

So, **H8**. Regulatory support will have a positive influence on cloud adoption.

Figure 1. The proposed model for cloud adoption in organizations



RESEARCH METHODS

There are two types of research methods that can be used in this exploratory study: qualitative and quantitative. A qualitative method allows participants to answer certain questions from their own perspectives. Qualitative data are generally collected using open-ended questions. In this method, researchers can obtain more information on the current situation, human attitudes, opinions and decisions (Tashakkori & Creswell, 2007). This approach can provide more in-depth information on the subject of the study (Anderson, 2010, 2010).

The second type of research method is a quantitative method. In this approach, data are collected through closed-ended questions and participants are not allowed to explain their responses (Tashakkori & Creswell, 2007). There are various ways to collect quantitative data, such as questionnaires and scientific experiments. Using this approach, researchers can measure participants' opinions and decisions and different strategies can be used to analyze numerical data (Venkatesh & Brown, 2013).

Mixed methods are a combination of quantitative and qualitative methods. By combining the two methods, researchers can gain more knowledge and more accurate results and provide a clearer picture of the problem (Venkatesh & Brown, 2013; ZHU, 2004). According to Mack, Woodsong, MacQueen, Guest, and Namey (2005) and Mack et al. (2005), some researchers have

used qualitative methods to gain an overview of the problem and an in-depth understanding of the results obtained using quantitative methods. In this study, different techniques can be used to collect qualitative and quantitative data.

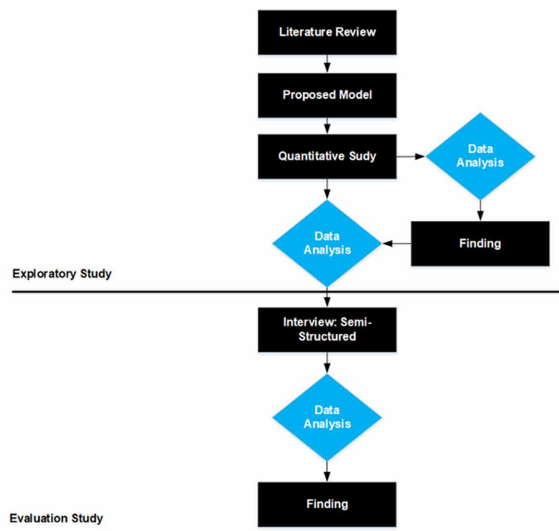
Our research focuses on various aspects that influence the adoption of cloud computing in information systems and its impact on IT agility. We have therefore chosen a research methodology that integrates several methods as shown in Figure 2. A combination of research methods, especially in both cases. Qualitative and quantitative paradigms have been proven in the IS discipline to be effective and contribute to a broad and deep understanding (cf. Kaplan & Duchon, 1988; Galliers, 1991; Lee, 1991; Landry & Banville, 1992; Mingers, 2001). The qualitative study was used to obtain additional information on the results of a quantitative study (Venkatesh & Brown, 2013).

Quantitative Methodology

Measurement Model

To assess theoretical constructions, a survey was conducted in the MENA region plus 10 large organizations in Europe (France, UK, Spain, Switzerland, and Germany) covering the manufacturing and service industries. A questionnaire was developed by a group of experts composed of experienced

Figure 2. Research design



researchers in the field of information systems. The questionnaire elements were based on published documentation Table 2. To be consistent with sources, constructions (agility, safety issues, cost savings, relative advantage, complexity, compatibility, technology readiness, senior management support, competitive pressure and regulatory support) were measured using a five-point Likert scale on a Likert scale at intervals ranging from “strongly disagree” to “strongly agree”.

The questionnaire was carried out in several stages. A first version has been developed to take into account the different theoretical assumptions. This first version has been tested with security managers and consultants. This pre-test allowed rephrasing certain questions to improve the comprehension of the questionnaire and to improve the quality of the given answers. The questionnaire was written in the three most widely spoken languages in the organizations, namely English, French, and Spanish.

Data Collect

As mentioned earlier, the focus of the field survey was a large organization in MENA region and ten organization in Europe. An online version of the questionnaire was sent by e-mail to qualified individuals (CIOs, IS directors and senior managers) in 400 manufacturing and service companies. Data were collected using an online questionnaire administered in two stages from mid-2017 to early 2018. The study used the “key informant” approach to data collection (Benlian & Hess, 2011) to identify the respondents in the organization who are most involved and knowledgeable about cloud computing. To target key informant respondents, we provided a clear description of cloud computing and examples. In order to increase the validity of the content, we indicated that the organization’s most familiar member should complete the survey. The final version of the questionnaire was written in English. Comprised 34 questions, in which each factor was measured by several elements. The participants’ demographics are shown in Table 3.

Results

The purpose of this study is to assess the determinants of cloud adoption, using a methodology that combines the innovative characteristics of cloud computing with the organization’s technological, organizational and environmental perspectives. We found that ten factors influence cloud adoption: agility,

Table 3. Participants' demographics

Variable		Frequency	Percentage
Organization size	100–500 employees	40	10%
	500–1000 employees	50	12.5%
	1000–2000 employees	80	20%
	More than 2000 employees	230	57.5%
Industry	Manufacturing	49	12.25%
	Petrochemical	10	2.5%
	Chemicals	62	15.5%
	Engineering	75	18.75%
	Energy	11	2.75%
	Financial services	87	21.75%
	IT	101	25.5%
	Retail	2	0.5%
	Other	3	0.75%
Market scope	International	260	65%
	Local	40	10%
	National	100	25%
Adoption stage	Yes	225	56.25%
	No	175	43.75%
Intend to adopt cloud services in the future	Yes	120	30%
	No	55	13.75%

Table 4. Summary of the factors that influence the adoption of cloud computing

Constructs	Items	Adapted source
Agility	A1 - Cloud computing allows you to manage your business activities in an efficient way.	(Yang et al., 2013)
	A2 - Cloud computing services improve the quality of operations.	
	A3 - Using cloud computing helps you get the job done faster at specific	
	A4 - The use of cloud computing offers new opportunities.	
Security concerns	S1 – Degree of company’s concern with data security on the cloud computing	(K. Zhu, Dong, et al., 2006), (Luo, Gurung, & Shim, 2010), (W.-W. Wu, 2011)
	S2 – Degree of concern for customers with data security in cloud computing	
	S3 – Degree of concern about privacy in cloud computing	
Cost savings	SC1 - Enterprise-level concerns about data security in cloud computing.	(Thiesse et al., 2011) (Sangle, 2011)
	SC2 - Level of customer concern about data security in cloud computing.	
	SC3 - Level of concern about privacy in cloud computing	

continued on following page

Table 4. Continued

Constructs	Items	Adapted source
Complexity	Cp1 - Using cloud computing requires lots of mental effort.	(Ifinedo, 2011) (Thiesse et al., 2011)
	Cp2 - Using cloud computing is frustrating.	
	Cp3 - Using cloud computing is too complex for business operations.	
	Cp4 - For firm employees, the skills required to adopt cloud computing are too complex.	
Compatibility	Ct1 - Cloud Computing can accommodate a company's work style.	(Ifinedo, 2011) (Thiesse et al., 2011)
	Ct2 - Cloud computing is fully compatible with today's business operations.	
	Ct3 - Cloud computing is compatible with your company's culture and value system.	
	Ct4 - Cloud computing will be compatible with existing company hardware and software.	
Technology readiness	Tc1 - Percentage of employees with Internet access.	(IFINEDO, 2011) ,(Oliveira & Martins, 2010)
	Tc2 - The company has knowledge of how IT can be used to support operations.	
	Tc3 - In the enterprise, there are the skills needed to implement cloud computing.	
Top management support	TS1 - Enterprise management supports the implementation of cloud computing.	(Chwelos, Benbasat, & Dexter, 1890) (Shah Alam, Ali, & Mohd. Jani, 2011) (Y. Zhu, Li, Wang, & Chen, 2010)
	TS2 - Company management demonstrates strong leadership and commitment to the process when it comes to information systems.	
	TS3 - Business leaders are prepared to take risks (financial and organizational) in the adoption of cloud computing.	
Firm size	FS1 – The number of company employees.	(K. Zhu et al., 2003), (Chwelos et al., 1890) , (Premkumar & Roberts, 1999)
	FS2 – Annual business volume.	
Competitive pressure	CP1 - The company believes that cloud computing can influence competition in their industry.	(IFINEDO, 2011) (Oliveira & Martins, 2010)
	CP2 - Competition is putting pressure on our site firm to adopt cloud computing.	
	CP3 - Some competitors have already started using cloud computing.	
Regulatory support	Re1 - There is a legal protection in the use of cloud computing.	(K. Zhu & Kraemer, 2005), (Shah Alam et al., 2011)
	Re2 - The legislation and regulations that exist today are effective in protecting the use of cloud computing.	
Cloud computing adoption	CA1 - In terms of cloud adoption, at what stage is your organization currently engaged in cloud adoption. I don't think about it; Being evaluated (e.g. as part of a pre-pilot study); Evaluating this technology, but not planning to adopt it; Evaluating and planning for adoption of this technology; Already adopted cloud computing services, infrastructure or platforms.	(Thiesse et al., 2011)
	CCA2 - If you think in future you will embrace cloud computing. How do you think that will happen? Do not consider; More than 5 years; Between 2 and 5 years; Between 1 and 2 years; Less than 1 year; Already-adopted Cloud Computing services, infrastructure or platforms.	

Note: All questions are based on a 5-point scale unless otherwise indicated.

Table 5. Mean and standard deviation of full and subsamples

Factors	Mean	SD
Agility	3.33	0.87
Security concerns	3.76	1.11
Cost savings	3.14	0.79
Complexity	2.26	0.80
Compatibility	2.90	0.80
Technology readiness	4.27	1.19
Top management support	2.89	0.96
Firm size	2.54	0.86
Competitive pressure	2.30	0.86
Regulatory support	2.58	0.85
Cloud computing adoption	2.40	1.61

complexity, Competitive pressure, technological readiness, senior management support, Regulatory, and firm size (Table 5). An integrative approach that combines innovation in cloud computing characteristics with organizational, technological, organizational and environmental perspectives. The findings indicate that five factors influence cloud adoption: Agility, complexity, technological readiness, senior management support and company size as shown in Table 5.

FINDING

Innovation Characteristics

Of the four innovation characteristics, Agility (H9) is positively influencing cloud-computing adoption. This finding is consistent with similar studies reported in the literature (Hsu et al., 2006; Tan & Ai, 2011; Y.-M. Wang, Wang, & Yang, 2010). The survey confirms that organizations realize the benefits of cloud computing agility. The benefits identified by the study include improved quality of business operations, faster task execution, increased productivity and the creation of new business opportunities.

With respect to the two variables that constitute advantages related to cloud technology, cost savings (H1b) are confirmed as the important factor to explain the relative advantage of cloud computing. This finding is consistent with

studies that have shown that cost savings are a powerful driver of cloud-based solutions adoption in sectors such in technology, manufacturing, financial, logistical, services and educational industries (Garrison, Kim, & Wakefield, 2012; Lyytinen v& Damsgaard, 2011; Benlian & Hess, 2011).

Security concerns (H1a) do not prevent cloud adoption. This can be explained by recent advances in privacy technologies, surveillance and encryption systems to ensure confidentiality, integrity and data protection in the cloud (Muñoz, Gonzalez, & Maña, 2012; Sonehara, Echizen, & Wohlgemuth, 2011; Wang, 2010). In addition, new federal standards and regulations such as the GDPR (Tankard & Pathways, 2016) and FedRamp (Montalbano, 2012). Act help build trust and organizational control over data when adopting cloud-based solutions. This can explain why security and privacy are not a concern when a cloud computing strategy is considered.

The compatibility (H3) is considered a factor facilitating the adoption of cloud computing for the service sector, but not significant for the manufacturing sector. Its importance in the service industry can be explained by the work style preferences and Internet business transactions that prevail among companies in this sector (Lee & Kim, 2007). In the case of manufacturing, the lack of importance of compatibility may be due to the nature of the applications (e.g., the important role of in-house software solutions such as resource planning software and computer controlled machining) and the limited requirements for Internet solutions in the industry (Grandon & Pearson, 2004; Ramdani, Kawalek, & Lorenzo, 2009). Therefore, the compatibility results are also mixed compared to previous research, and further research is needed to reach a definitive conclusion.

In addition, the complexity factor (H2) is a barrier to the adoption of cloud computing in the service sector. The concept of complexity associated with cloud computing is no different from other disruptive technologies and appears to be an important deterrent to the adoption of cloud computing. Complexity can be associated with perceived change, which is known to be an unsatisfactory and frustrating source (Kets de Vries & Balazs, 1998). The results indicate that complexity is not a blocking factor for firms in the manufacturing sector. Complexity has been judged insignificant by some researchers (Low et al., 2011), while others have said the opposite (Borgman, Bahli, Heier, & Schewski, 2013). As a result, previous studies are not clear-cut on the role of complexity, implying that further researches are needed before precise conclusions can be reached.

Technology Readiness

Technology readiness (H4) is a driver for cloud computing adoption. According to the study, companies with an established technology infrastructure and a technically skilled workforce will be better suited to integrating cloud computing. However, our study indicates that the implementation of cloud computing can disrupt services and create management challenges in both IT and non-IT organizations. The finding indicates that organizations must ensure that the technology infrastructure and availability of IT specialists are adequate for integrating cloud solutions into business operations with minimal downtime. Unlike previous studies, which have suggested that technological readiness does not necessarily influence cloud adoption (Low et al., 2011). And that technological readiness is not relevant for technology companies (Y. Wu et al., 2013), and that for organizations with the capacity to more information processing is less apt to embrace cloud computing.

Organizational Context

In our study, we found empirically that (H5) top management support is important in explaining the adoption of cloud computing. According to the results of the study, senior management has an influence on the adoption of cloud computing by demonstrating its support through the commitment of financial and organizational resources and by engaging in the process. These findings are consistent with the results of previous research on technology adoption and use (Ifinedo, 2011; Luo et al., 2010; Ramdani et al., 2009).

The enterprise size factor (H6) is a predictive variable of cloud adoption. This conclusion is consistent with the literature that large firms have the necessary resources needed to address investment risk and cost associated related to emerging technology (A. Y. L. Chong & Chan, 2012; Crook & Kumar, 1998; Y.-M. Wang et al., 2010). In contrast, small businesses generally lack the resources to build knowledge and to implement and test cloud computing (Thiesse et al., 2011).

The enterprise size factor (H6) is a predictive variable of cloud adoption. This conclusion is consistent with the literature that large firms have the necessary resources needed to address investment risk and cost associated related to emerging technology (A. Y. L. Chong & Chan, 2012; Crook & Kumar, 1998; Y.-M. Wang et al., 2010). In contrast, small businesses

generally lack the resources to build knowledge and to implement and test cloud computing (Thiesse et al., 2011).

Environmental Context

Few studies have addressed the importance of the environmental context of cloud computing. According to Low et al. (2011), competitive pressure has pushed high-tech companies to adopt cloud computing more quickly. Also, (IFINEDO, 2011) has determined that competitive pressure has a positive impact on the adoption of technologies that support e-commerce. While pressures from customers, business partners and government support have not played a significant role.

DISCUSSION AND INTERPRETATIONS

Results of our survey indicate the two variables in the environmental context, the pressure of competition and regulatory support are not determinative of cloud adoption. firms are likely to be aware of cloud benefits, but specific technology factors and organizational contexts prevent cloud benefits from translating to a competitive advantage. It was also found that regulatory support for cloud computing adoption was not available at significant. This does not necessarily mean that firms do not take into account current standards and regulations, on the contrary, legislation protecting the use of cloud computing has not been seriously adopted by the organization's decision makers. Regulatory processes are essential to instilling the confidence needed at firms to turn innovation into business opportunities. Without commercially sound economic incentives, technological advances, evolving cloud standards and federal regulations may not be able to overcome the barriers to cloud adoption.

The findings of our study suggest that agility, complexity, support from senior management, enterprise size and technological readiness, influence adoption of cloud computing by enterprises.

Qualitative Study

The second study focuses more on how cloud computing affects the agility of information systems. Data were collected through semi-structured interviews with about 20 computer experts working in 10 large organizations in Europe

(France, UK, Spain, Switzerland, and Germany) that have already adopted cloud technology.

The Sample Size

It was important to identify the sample size before conducting this study. In order to determine the minimum sample size, G*Power software was used. G*Power is software that enables researchers to compute the required sample size and increase the accuracy of their results (Bourque & Fielder, 2003). The parameters identified to compute the minimum sample size were as follows:

- **Effect Size:** According to Faul, Erdfelder, Lang, and Buchner (2007), there are three parameters of effect size small, medium and large. The appropriate effect size for this exploratory study is 0.8 (i.e., large).
- Type I error, also known as alpha (α for 95% confidence level $\alpha = 0.05$). This means the probability of rejecting the null hypothesis when it is true is 5% (0.05). Type one error means false rejection of the null hypothesis.
- Type II error (i.e., $1-\beta$ err prob): Type two error indicates that the null hypothesis will not be rejected when it is actually false (Banerjee, Ghosh, & Banerjee, 2012). In other words, type two error means false acceptance of the null hypothesis. This is conventionally set at 20%.; so ($1-\beta$ err prob) = 0.8.

In this study, the calculation was performed under a t-test family (one sample case). The results indicated that the minimum sample size for the questionnaire was fifteen participants. Table 6 illustrates the statistical calculation of the sample.

Table 6. Sample size calculation using the G power software*

Statistical test	Means: Difference from constant (one sample case)
Tails	Two
Effect size d	0.8
α error prob.	0.05
Power ($1-\beta$ err prob)	0.8
Minimum sample size	15

In terms of interviews, there is no typical sample size for data collection from interviews; thus, there is no set number for participants in interviews. However, Tashakkori and Creswell (2007), recommends that from 5 to 25 interviewees is acceptable, while Morse (1994) suggests that six is the minimum for participants in interviews. Furthermore, Thomson (2010) conducted a review of one hundred studies regarding sample size in interviews and found that the point at which any increase in a number of interviews will lead to repeated material and data saturation occurs between 10 and 30 interviews (Thomson, 2010). Strauss and Corbin (1998) also state that the saturation of data is dependent on a researcher's decision. In this present study, the researcher has taken into account these suggestions and conducted interviews until there was no new data to be added to the study.

Interview Design

The purpose of the semi-structured interviews was to examine the extent to which the adoption of cloud computing will increase information systems agility. Interview questions were prepared prior to the interviews and included closed and open-ended questions. According to Foddy and Foddy (1994), the five-point Likert scale is the optimal choice for cases that require decisions; (Lietz, 2008) also mentioned that this scale can increase reliability and validity of results. Therefore, in this study the closed-ended questions were designed using a five-point Likert scale: (very important = 5; important = 4; may be important = 3; not important = 2 and not relevant = 1). The other questions were open, which helped the researcher to understand an organization's requirements and attitude toward cloud adoption. Table 7 presents an outline of the interview questions. The interview questions are developed in English to verify the clarity of the questions. Adjustments based on the pilot interviews were made to the interview questions, including rephrasing and deleting some inaccurate questions.

Questionnaire Design

To confirm the proposed cloud adoption model, a self-administered questionnaire was developed for this study. The purpose of the questionnaire was to confirm the factors that already exist in the cloud adoption model, as well as other factors that were identified in interviews with IT experts. The questionnaire was divided into two sections: demographic information

Table 7. The interview questions

Number	Questions
Q1	Cloud computing has enabled you to manage your business activities efficiently. Using cloud computing offers new benefits?
Q2	Cloud computing services improve the quality of operations?
Q3	Does your organization adopt cloud computing?
Q4	Using cloud-computing helps you get the job done faster to is more efficient.
Q5	What are the challenges that your organization faced with using cloud computing?

and 28 closed-ended questions concerning seventeen factors. These factors are security, relative advantage, agility, compatibility, complexity, senior management support, organizational size, technological readiness, regulatory compliance, and competitive pressure. The reason there were 28 closed-ended questions was that some factors were measured by more than one question. For example, Agility has two questions, one measuring the impact of Agility on cost by predicting changes and the other on responsiveness. Closed-ended questions were designed based on interview results and using a five-point Likert scale: (strongly agree = 5; agree = 4; neutral = 3; neutral = 3; disagree = 2 and strongly disagree = 1): The questions used were as follows:

The Results of the Interviews

The data were collected using semi-structured interviews with twenty IT experts working in different private organizations. The aim of this stage of the research was to review the factors identified previously in Table 2.

Demographic Information

The interviews were conducted with twenty IT experts at different organizations in MENA region. All the participants were working in IT departments in different sectors (such as manufacturing, engineering and energy), in large organizations and SMEs. All participants had at least five years' working experience, so they had the ability to understand the current situation of their organization and future trends. The interviews were carried out between March and May 2018, at the experts' workplaces (i.e., face-to-face interviews), and they were recorded using a recording device with the permission of the experts. Seven of the participants in this study are working in companies that already

Table 8. Participants' demographics

	Variable	Frequency	Percentage
Organization size	100–500 employees	4	13.3%
	500–1000 employees	6	20%
	1000–2000 employees	12	40%
	More than 2000 employees	8	26.7%
Industry	Manufacturing	4	13.3%
	Petrochemical	4	13.3%
	Chemicals	3	10%
	Engineering	7	23.3%
	Energy	1	3.3%
	Financial services	2	6.7%
	IT	4	13.3%
	Retail	2	6.7%
	Other	3	10%
Market scope	International	22	73.3%
	Local	2	6.7%
	National	6	20%

have adopted cloud computing while thirteen (65%) of them are not. Table 8 presents more information about organizations participating in this interview.

The purpose of the questionnaire was to confirm which factors influence an organization's decision to use cloud services. The SPSS software was used to analyze data collected from IT staff working in different private organisations in the MENA region.

Parametric tests analyze measured data by scale and interval ratio, while nonparametric tests analyze ordinal and classified data. Overall, parametric tests are more flexible and powerful than non-parametric tests, and are therefore preferred by most researchers. Therefore, the data collected were tested using the parametric test (t-test on a sample) and the test value was defined as 3 on the five-point Likert scale, which ranged from 5 (strongly agree) to 1 (strongly disagree). Table 9 illustrates the results of the questionnaire analysis.

Hypothesis

In the aim to response a second research question, the following assumptions were made and tested at a 90% confidence level. The hypotheses (H1) include

Managing the Cloud for Information System Agility in Organizations

Table 9. A framework for cloud computing’s impact on information systems agility

Factors		Statements	Mean	Sig. (2-tailed)
IT Agility	Application Agility	The organization will have the capacity to add a new product or service with efficiency. In this aims organization.	4.67	<0.001
	Information Agility	- Organization needs to improve the sharing of application data for all stakeholders and organization partners. - An employee will have a possibility to quickly access to the data of the applications and the possibility of recovering them rapidly.	4.60	<0.001
	Compatibility & interoperability	Organization will need to deploy an application migration process, to link the local environment to the cloud environment while maintaining a level of security.	3.60	0.004
	Elasticity	Organization must manage these expansions to the growing demand of customers and have the ability to accelerate the necessary increase in bandwidth allocation and computing resources from the cloud service provider.	3.90	<0.001
IT Process Agility	Maintenance Process Agility	Ability to adapt to change in information systems through system development, implementation, modification and maintenance activities. An organization with such IT agility can effectively modify its system, enabling it to respond more effectively to changing market opportunities.	4.03	<0.001
	Planning Process Agility	Reduction of time and effort for application support and maintenance. The integration of new branches in the company must be less complex. The IT should easily assess and prioritize proposed changes.	3.23	0.257
	Monitoring & Assessment Process Agility	Recall that the relevant forces of environmental change include competitor actions, strategic changes, and changes in consumer preferences or IS staff skills, economic changes, regulatory and legal changes, and technological advances. These different changes require a standby to detect any potential changes regarding each of these types.	4.17	<0.001
Human Agility	Training & Staff	- Conducted training and internships for IT staff to manage different systems and applications. - IT staff will have the ability to translate business problems into technical solution.	4.73	<0.001
	Business and Technical Skill	IT staff should have the ability to deal with unexpected changes and efficiency seize emerging opportunities.	4.47	<0.001
Business Agility	Response	The use of cloud computing increases the organization’s ability to cope with unexpected changes (i.e., unexpected events such as corrections and reconfigurations).	4.53	<0.001
	Customer service	Organizational mechanisms must be able to support service delivery that meets client needs.	4.13	<0.001
	Competitive status	The ability to remain competitive by providing answers under any conditions will seize new opportunities and remain competitive.	4.53	<0.001

the different associations between agility categories and cloud computing models formulated as follows:

H1: There is an association between the use of a software model as a cloud service model and the improvement of the IS Agility category where the

cloud model is either (IaaS, PaaS or SaaS) and the IS Agility category is either (Technical Infrastructure Agility, IT Processes Agility, Human Characteristics, or Business Aspects).

RESULTS

The following section summarizes these findings. Figure 3 and Figure 4 illustrate the usage frequencies and percentages for various cloud computing service models and deployment models. Figure 3 shows answers to aggregated categories of IS agility.

As can be seen in Figure 3 and Figure 4, the percentage of usage is mainly attributable to infrastructure as a service within the private cloud. In addition, an interesting observation in Figure 5 includes the high percentage of responses in the business agility category, including: greater user confidence to faced unexpected changes (i.e., unexpected events such as fixes and re-configurations), greater satisfaction with efficiency and effectiveness in seizing emerging opportunities, and a positive contribution of using clouds to align IT strategies with business strategies.

Figure 5 shows the responses to the aggregated categories of IS agility.

Figure 3. Cloud usage by type

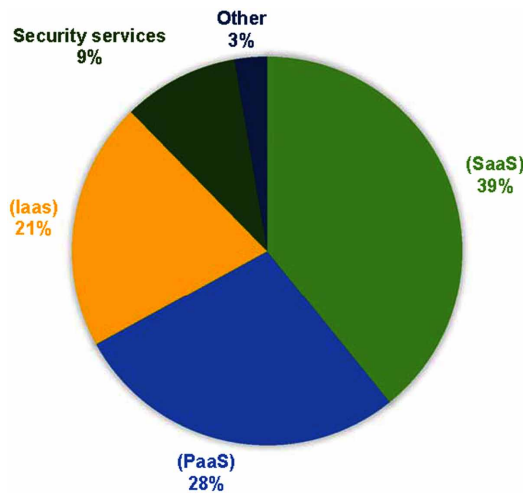


Figure 4. Cloud usage by deployment model

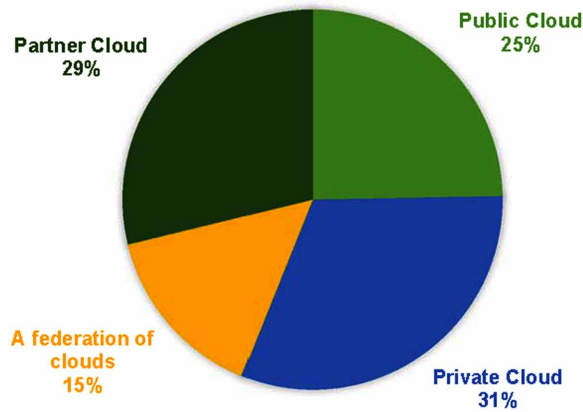
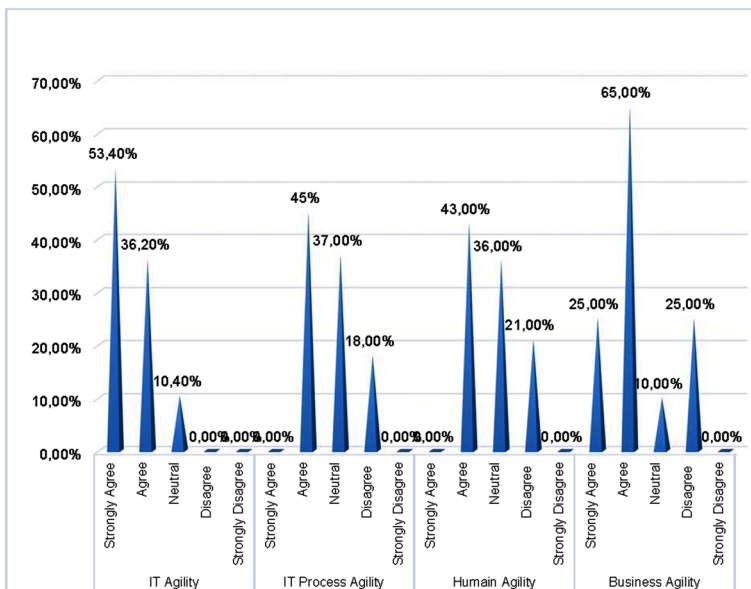


Figure 5. Combined frequency distributions for responses to aggregated IS agility categories



Result Discussion

The cloud is a service delivery issue: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS). In other words, the cloud provides a set of computing resources that function efficiently as a

single computer. However, as the results of the statistical analysis show, not all of these services have a direct association with agility as perceived by IT professionals. More specifically, the PaaS Cloud model enables users to respond more effectively to business demands and helps ensure employees have on-demand access to critical business information, customers, partners and each other, using virtually any device, from virtually anywhere and from anywhere. Therefore, users can give priority to the most critical business tasks first.

However, IaaS focuses more on reducing the burden of managing anticipation and building excess IT infrastructure, resulting in reduced management, maintenance and deployment time, with the added benefit of greater scalability to more easily manage peak demand, studies have also shown the lack of association between SaaS and any category of agility. This conclusion is supported by the fact that SaaS is seen more as an economic option than an improvement in agility. Unlike conventional financial models of software vendors that rely on license fees to support their profits and losses, SaaS allows users to pay only for what is used during a given period while being much less dependent on local IT staff and services, which would increase some limits on agility in general.

Surveys indicate that there is an improvement in user confidence in the face of unexpected changes, efficiency and effectiveness of taking advantage to emerge opportunities and aligning IT strategies with business strategies. Additionally, cloud computing has allowed organizations to reduce the time and effort spent on support and maintenance, decrease efforts to assess and prioritize proposed changes, facilitate capacity planning and performance information collection, and simplify service management.

CONCLUSION

Cloud computing is an important evolution of IS technology. It boasts attractive properties such as agility, scalability, pay-per-use, and cost efficiency. This study sought to identify the determinants of cloud-computing adoption based on innovation characteristics and the technology, organization, and environmental contexts of organizations, and evaluate how cloud computing changes IS agility, it started. A research model was developed that integrates the DOI theory and the TOE framework. The model was empirically evaluated based on a semi-structured interview with IT experts. It was used to compare the adoption of cloud computing in two distinct sectors, namely

manufacturing and services. The results indicated that Agility, relative advantage, complexity, technological readiness, top management support, and firm size have a direct effect on a firm's adoption of cloud computing. The analysis of results validated the direct effect of Agility on cloud-computing adoption. In addition, we compiled four groups of attributes into a framework proposed for consideration in the consideration of IS agility, A survey was built based on Agility attributes. The data were collected from employees of 10 on a sample of 10 different large companies in Europe (France, UK, Spain, Switzerland, and Germany). Drawing on research findings, we concluded that some cloud computing service models improve specific dimensions of agility, for example, IaaS increases technical infrastructure agility. PaaS improves human characteristics while SaaS does not associate with any category.

For decision makers in the organization who are considering cloud-based initiatives, our results provide a solid foundation for assessing the direct and indirect effects of cloud computing innovation features and the literature related to its adoption in various industries.

Our Results also indicate that cloud computing will increase the agility of information systems which allows the company to realize cost savings resulting from reduced IT capital expenditures, reduced negotiation costs and reduced maintenance and energy costs The benefits of environmental responsibility by reducing environmental impacts through the adoption of cloud computing.

In general, it seems that cloud computing brings improvement to the agility aspects of the information systems of organizations that adopt cloud computing technology specifically SaaS.

The last section of this book will include 3 chapters that will deal with information security governance practices, frameworks and policies in large organizations

REFERENCES

Abdollahzadehgan, A., Che Hussin, A. R., Gohary, M. M., & Amini, M. (2013). The Organizational Critical Success Factors for Adopting Cloud Computing in SMEs. *Journal of Information Systems Research and Innovation*, 4(1), 67–74.

Adams, D. A., Nelson, R. R., Todd, P. A., Ahmi, A., Kent, S., Al-Ansi, A. A., ... Willborn, W. W. (2009). Factors Affecting the Adoption of Open Systems: An Exploratory Study. *Management Information Systems Quarterly*, *16*(2), 1521–1552. doi:10.1108/02686900510606092

Adamson, G., Wang, L., Holm, M., & Moore, P. (2017). Cloud manufacturing—a critical review of recent development and future trends. *International Journal of Computer Integrated Manufacturing*, *30*(4–5), 347–380. doi:10.1080/0951192X.2015.1031704

Alam, S. S. (2009). Adoption of internet in Malaysian SMEs. *Journal of Small Business and Enterprise Development*, *16*(2), 240–255. doi:10.1108/14626000910956038

Altaf, F., & Schuff, D. (2010). Taking a flexible approach to ASPs. *Communications of the ACM*, *53*(2), 139–143. doi:10.1145/1646353.1646389

Anderson, C. (2010). Presenting and evaluating qualitative research. *American Journal of Pharmaceutical Education*, *74*(8), 141. doi:10.5688/aj7408141 PMID:21179252

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... Rabkin, A. (2010). A View of Cloud Computing Clearing the clouds away from the true potential and obstacles posed by this computing capability. *Communications of the ACM*, *53*(4), 50–58. doi:10.1145/1721654.1721672

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... Zaharia, M. (2010). A View of Cloud Computing. *Communications of the ACM*, *53*(4), 50–58. doi:10.1145/1721654.1721672

Avram, M. G. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, *12*, 529–534. doi:10.1016/j.protcy.2013.12.525

Azadegan, A., & Teich, J. (2010). Effective benchmarking of innovation adoptions: A theoretical framework for e-procurement technologies. *Benchmarking: An International Journal*, *17*(4), 472–490. doi:10.1108/14635771011060558

Banerjee, A., Ghosh, S. C., & Banerjee, N. (2012). Pack Your Sack for the Cloud. In *Proceedings of the 5th India Software Engineering Conference* (pp. 116–157). New York: ACM. 10.1145/2134254.2134283

- Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems*, 52(1), 232–246. doi:10.1016/j.dss.2011.07.007
- Bhat, J. M. (2013). Adoption of cloud computing by SMEs in India: A study of the institutional factors. *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime, 1*, 271–278.
- Bishop, M. (2002). Computer Security: Art and Science. *Bioinformatics and Biomedical Engineering, 2008. ICBBE 2008. The 2nd International Conference on*. 10.1002/ejoc.201200111
- Borgman, H. P., Bahli, B., Heier, H., & Schewski, F. (2013). Cloudrise: Exploring cloud computing adoption and governance with the TOE framework. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 4425–4435. 10.1109/HICSS.2013.132
- Bourque, L., & Fielder, E. P. (2003). *How to conduct self-administered and mail surveys* (Vol. 3). Sage. doi:10.4135/9781412984430
- Brinda, M., & Heric, M. (2017). *The Changing Faces of the Cloud*. Bain & Company. Bain & Company.
- Buxmann, P., Diefenbach, H., & Hess, T. (2015). Cloud Computing. *Die Softwareindustrie*, 221–256. doi:10.1007/978-3-662-45589-0_7
- Cervone, H. F. (2010). An overview of virtual and cloud computing. *OCLC Systems & Services: International Digital Library Perspectives*, 26(3), 162–165. doi:10.1108/10650751011073607
- Chang, V., De Roure, D., Wills, G., & Walters, R. J. (2011). Case Studies and Organisational Sustainability Modelling Presented by Cloud Computing Business Framework. *International Journal of Web Services Research*, 8(3), 26–53. doi:10.4018/jwsr.2011070102
- Changchit, C., & Chuchuen, C. (2018). Cloud computing: An examination of factors impacting users' adoption. *Journal of Computer Information Systems*, 58(1), 1–9. doi:10.1080/08874417.2016.1180651
- Chong, A. Y. L., & Chan, F. T. S. (2012). Structural equation modeling for multi-stage analysis on Radio Frequency Identification (RFID) diffusion in the healthcare industry. *Expert Systems with Applications*, 39(10), 8645–8654. doi:10.1016/j.eswa.2012.01.201

- Chong, A. Y.-L., Ooi, K.-B., Lin, B., & Raman, M. (2009). Factors Affecting the Adoption Level of C-Commerce: An Empirical Study. *Journal of Computer Information Systems*, 50(2), 13–22. doi:10.1080/08874417.2009.11645380
- Chong, S., & Bauer, C. (2000). *A Model of Factor Influences on Electronic Commerce Adoption and Diffusion in Small-and Medium-sized Enterprises*. Association for Information Systems AIS Electronic Library (AISeL).
- Chwelos, P., Benbasat, I., & Dexter, A. S. (1890). Empirical Test of an EDI Adoption Model Empirical Test of an EDI Adoption Model. *Information Systems Research*, 2(604), 304–321.
- Crook, C. W., & Kumar, R. L. (1998). Electronic data interchange: A multi-industry investigation using grounded theory. *Information & Management*, 34(2), 75–89. doi:10.1016/S0378-7206(98)00040-8
- Dedrick, J., & West, J. (2004). An exploratory study into open source platform adoption. *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the, 0(C)*. 10.1109/HICSS.2004.1265633
- Dillon, T., Wu, C., & Chang, E. (2010). Cloud Computing: Issues and Challenges. *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, 27–33. 10.1109/AINA.2010.187
- Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, 39(2), 175–191. doi:10.3758/BF03193146 PMID:17695343
- Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. *Future Generation Computer Systems*, 29(1), 84–106. doi:10.1016/j.future.2012.05.023
- Fichman, R. (2004). Going Beyond the Dominant Paradigm for Information Technology Innovation Research : Emerging Concepts. *Journal of the Association for Information Systems*, 5(8), 314–355. doi:10.17705/1jais.00054
- Foddy, W., & Foddy, W. H. (1994). *Constructing questions for interviews and questionnaires: Theory and practice in social research*. Cambridge University Press.
- Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). Cloud Computing and Grid Computing 360-degree compared. *Grid Computing Environments Workshop, GCE 2008*. 10.1109/GCE.2008.4738445

Garrison, G., Kim, S., & Wakefield, R. L. (2012). Success factors for deploying cloud computing. *Communications of the ACM*, 55(9), 62. doi:10.1145/2330667.2330685

Ghobakhloo, M., Arias-Aranda, D., & Benitez-Amado, J. (2011). Adoption of e-commerce applications in SMEs. *Industrial Management and Data Systems* (Vol. 111). doi:10.1108/02635571111170785

Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010). The Characteristics of Cloud Computing. In *2010 39th International Conference on Parallel Processing Workshops* (pp. 275–279). Academic Press. 10.1109/ICPPW.2010.45

Goscinski, A., & Brock, M. (2010). Toward dynamic and attribute based publication, discovery and selection for cloud computing. *Future Generation Computer Systems*, 26(7), 947–970. doi:10.1016/j.future.2010.03.009

Goyal, A., & Dadizadeh, S. (2009). A survey on cloud computing. *Technical Report for CS*, 58(December), 55–58. doi:10.17148/IJARCCCE.2016.54261

Grandon, E. E., & Pearson, J. M. (2004). Electronic commerce adoption: An empirical study of small and medium US businesses. *Information & Management*, 42(1), 197–216. doi:10.1016/j.im.2003.12.010

Greenhalgh, T., Robert, G., MacFarlane, F., Bate, P., & Kyriakidou, O. (2004). Diffusion of Innovations in Service Organizations: Systematic Review and Recommendations. *The Milbank Quarterly*, 82(4), 581–629. doi:10.1111/j.0887-378X.2004.00325.x PMID:15595944

Hoberg, P., Wollersheim, J., & Krcmar, H. (2012). The Business Perspective on Cloud Computing-A Literature Review of Research on Cloud Computing. *AMCIS 2012 Proceedings*, Paper 5.

Hsu, P.-F., Kraemer, K. L., & Dunkle, D. (2006). Determinants of E-Business Use in U.S. Firms. *International Journal of Electronic Commerce*, 10(4), 9–45. doi:10.2753/JEC1086-4415100401

Ifinedo, P. (2011). Internet/e-business technologies acceptance in Canada's SMEs: An exploratory investigation. *Internet Research*, 21(3), 255–281. doi:10.1108/10662241111139309

Ifinedo, P. (2011). An empirical analysis of factors influencing internet/e-business technologies adoption by SMEs in Canada. *International Journal of Information Technology & Decision Making*, 10(4), 731–766. doi:10.1142/S0219622011004543

Kalle, L., & M., R. G. (2003). Disruptive information system innovation: the case of internet computing. *Information Systems Journal*, 13(4), 301–330.

Kets de Vries, M. F. R., & Balazs, K. (1998). Beyond the quick fix: The psychodynamics of organizational transformation and change. *European Management Journal*, 16(5), 611–622. doi:10.1016/S0263-2373(98)00037-1

Kim, K. H., Beloglazov, A., & Buyya, R. (2009). Power-aware Provisioning of Cloud Resources for Real-time Services. In *Proceedings of the 7th International Workshop on Middleware for Grids, Clouds and e-Science* (p. 1:1-1:6). New York: ACM. 10.1145/1657120.1657121

Kim, W. (2009). Cloud computing: Status and prognosis. *Journal of Object Technology*, 8(1), 65–72. doi:10.5381/jot.2009.8.1.c4

Klein, R. (2012). Assimilation of Internet-based purchasing applications within medical practices. *Information & Management*, 49(3), 135–141. doi:10.1016/j.im.2012.02.001

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37(4), 372–386. doi:10.1016/j.telpol.2012.04.011

Kuan, K. K. Y., & Chau, P. Y. K. (2001). A perception-based model for EDI adoption in small businesses using a technology–organization–environment framework. *Information & Management*, 38(8), 507–521. doi:10.1016/S0378-7206(01)00073-8

Kunio, T. (2010). NEC cloud computing system. *NEC Technical Journal*, 5(2), 10–15.

Lee, S., & Kim, K. (2007). Factors affecting the implementation success of Internet-based information systems. *Computers in Human Behavior*, 23(4), 1853–1880. doi:10.1016/j.chb.2005.12.001

Lietz, P. (2008). *Questionnaire design in attitude and opinion research: Current state of an art*. Citeseer.

- Lim, K. H. (2009). Knowledge management systems diffusion in Chinese enterprises: A multistage approach using the technology-organization-environment framework. *Journal of Global Information Management*, 17(1), 70–84. doi:10.4018/jgim.2009010104
- Lin, A., & Chen, N.-C. (2012). Cloud computing as an innovation: Perception, attitude, and adoption. *International Journal of Information Management*, 32(6), 533–540. doi:10.1016/j.ijinfomgt.2012.04.001
- Lin, H.-F., & Lin, S.-M. (2008). Determinants of e-business diffusion: A test of the technology diffusion perspective. *Technovation*, 28(3), 135–145. doi:10.1016/j.technovation.2007.10.003
- Lippert, S. K., & Govindrajulu, C. (2006). Technological, Organizational, and Environmental Antecedents to Web Services Adoption. *Communications of the IIMA*, 6(1), 146–158. doi:10.1017/CBO9781107415324.004
- Lohr, B. S. (2007). Google and I. B. M. Join in Cloud Computing Research. New York, 9–10.
- Low, C., Wu, M., & Chen, Y. (2011). Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems*, 111(7), 1006–1023. doi:10.1108/02635571111161262
- Luo, X., Gurung, A., & Shim, J. P. (2010). Understanding the determinants of user acceptance of enterprise instant messaging: An empirical study. *Journal of Organizational Computing and Electronic Commerce*, 20(2), 155–181. doi:10.1080/10919391003709179
- Lyytinen, K., & Damsgaard, J. (2011). Inter-organizational information systems adoption—a configuration analysis approach. *European Journal of Information Systems*, 20(5), 496–509. doi:10.1057/ejis.2010.71
- Mack, N., Woodson, C., MacQueen, K. M., Guest, G., & Namey, E. (2005). *Qualitative research methods: a data collectors field guide*. Academic Press.
- Marston, S., Bandyopadhyay, S., & Ghalsasi, A. (2011). Cloud Computing - The Business Perspective. *2011 44th Hawaii International Conference on System Sciences*, 1–11. doi:10.1109/HICSS.2011.102
- Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing - The business perspective. *Decision Support Systems*, 51(1), 176–189. doi:10.1016/j.dss.2010.12.006

- Martens, B., & Teuteberg, F. (2012). Decision-making in cloud computing environments: A cost and risk based approach. *Information Systems Frontiers*, 14(4), 871–893. doi:10.1007/10796-011-9317-x
- Mazhelis, O., & Tyrväinen, P. (2012). Economic aspects of hybrid cloud infrastructure: User organization perspective. *Information Systems Frontiers*, 14(4), 845–869. doi:10.1007/10796-011-9326-9
- Metheny, M. (2013). Federal Cloud Computing. *Federal Cloud Computing*, 71–102. doi:10.1016/B978-1-59-749737-4.00004-6
- Misra, S. C., & Mondal, A. (2011). Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment. *Mathematical and Computer Modelling*, 53(3–4), 504–521. doi:10.1016/j.mcm.2010.03.037
- Montalbano, E. (2012). Feds refine cloud security standards. *Information Week*.
- Morse, J. M. (1994). *Designing funded qualitative research*. Academic Press.
- Muñoz, A., Gonzalez, J., & Maña, A. (2012). A Performance-Oriented Monitoring System for Security Properties in Cloud Computing Applications. *The Computer Journal*, 55(8), 979–994. doi:10.1093/comjnl/bxs042
- Nkhoma, M. Z., & Dang, D. P. T. (2013). Contributing Factors of Cloud Computing Adoption : A Technology - Organisation - Environment Framework Approach. *International Journal of Information Systems and Engineering*, 1(1), 38–49.
- Nkhoma, M. Z., Dang, D. P. T., & De Souza-Daw, A. (2013). Contributing factors of cloud computing adoption: a technology-organisation-environment framework approach. In *Proceedings of the European Conference on Information Management & Evaluation* (pp. 180–189). Academic Press.
- Oliveira, T., & Martins, M. F. (2010). Understanding e-business adoption across industries in European countries. *Industrial Management & Data Systems*, 110(9), 1337–1354. doi:10.1108/02635571011087428
- Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *The Electronic Journal Information Systems Evaluation*, 14(1), pp 110-121.

- Phan, D. H., Suzuki, J., Carroll, R., Balasubramaniam, S., Donnelly, W., & Botvich, D. (2012). Evolutionary Multiobjective Optimization for Green Clouds. In *Proceedings of the 14th Annual Conference Companion on Genetic and Evolutionary Computation* (pp. 19–26). New York: ACM. 10.1145/2330784.2330788
- Premkumar, G., & Roberts, M. (1999). Adoption of new information technologies in rural small businesses. *Omega*, 27(4), 467–484. doi:10.1016/S0305-0483(98)00071-1
- Ramdani, B., Kawalek, P., & Lorenzo, O. (2009). Predicting SMEs' adoption of enterprise systems. *Journal of Enterprise Information Management*, 22(1/2), 10–24. doi:10.1108/17410390910922796
- Rimienė, K. (2011). Supply chain agility concept evolution (1990-2010). *Economics & Management*, 16.
- Ringle, C. M., Sinkovics, R. R., & Henseler, J. (2009). The use of partial least squares path modeling in international marketing. In *New Challenges to International Marketing* (Vol. 20, pp. 277–319). Emerald Group Publishing Limited.
- Rogers, E. M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.
- Sangle, S. (2011). Adoption of cleaner technology for climate proactivity: A technology–firm–stakeholder framework. *Business Strategy and the Environment*, 20(6), 365–378.
- Schneiderman, R. (2011). For Cloud Computing, the Sky Is the Limit. *IEEE Signal Processing Magazine*, 28(1), 15–144. doi:10.1109/MSP.2010.938751
- Shah Alam, S., Ali, M. Y., & Mohd. Jani, M. (2011). An Empirical Study of Factors Affecting Electronic Commerce Adoption among SMEs in Malaysia. *Journal of Business Economics and Management*, 12(2), 375–399. doi:10.3846/16111699.2011.576749
- Shen, Z., & Tong, Q. (2010). The security of cloud computing system enabled by trusted computing technology. In *Signal Processing Systems (ICSPS), 2010 2nd International Conference on* (Vol. 2, pp. V2--11). IEEE.
- Siegel, J., & Perdue, J. (2012). Cloud services measures for global use: the service measurement index (SMI). In *SRII Global Conference (SRII), 2012 Annual* (pp. 411–415). IEEE. 10.1109/SRII.2012.51

Sila, I. (2010). Do organisational and environmental factors moderate the effects of Internet-based interorganisational systems on firm performance? *European Journal of Information Systems*, 19(5), 581–600. doi:10.1057/ejis.2010.28

Sitaram, D., & Manjunath, G. (2012). Moving To The Cloud. *Moving To The Cloud*, 2(1), 1–10. doi:10.1016/C2010-0-66389-9

Smith, D. M. (2017). *Gartner Insights on How and Why Leaders Must Implement Cloud Computing Cloud Strategy Leadership Have you or your CIO expressed any of these concerns?* Gartner.

Sonehara, N., Echizen, I., & Wohlgemuth, S. (2011). Isolation in cloud computing and privacy-enhancing technologies: Suitability of privacy-enhancing technologies for separating data usage in business processes. *Business & Information Systems Engineering*, 3(3), 155–162. doi:10.1007/12599-011-0160-x

Stanoevska, K., Wozniak, T., & Ristol, S. (2009). *Grid and cloud computing: a business perspective on technology and applications*. Springer Science & Business Media.

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Procedures and techniques for developing grounded theory*. Thousand Oaks, CA: Sage.

Sultan, N. (2010). Cloud computing for education: A new dawn? *International Journal of Information Management*, 30(2), 109–116. doi:10.1016/j.ijinfomgt.2009.09.004

Tan, X., & Ai, B. (2011). The issues of cloud computing security in high-speed railway. In *Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on* (Vol. 8, pp. 4358–4363). IEEE.

Tankard, C., & Pathways, D. (2016). What the GDPR means for. *Network Security*, 2016(6), 5–8. doi:10.1016/S1353-4858(16)30056-3

Tashakkori, A., & Creswell, J. W. (2007). Article. *Journal of Mixed Methods Research*, 3–7. doi:10.1177/2345678906293042

Thiesse, F., Staake, T., Schmitt, P., & Fleisch, E. (2011). The rise of the “next-generation bar code”: An international RFID adoption study. *Supply Chain Management*, 16(5), 328–345. doi:10.1108/13598541111155848

Thomas, M. A., Redmond, R. T., & Weistroffer, H. R. (2009). Moving to the cloud: Transitioning from client-server to service architecture. *Journal of Service Science*, 2(1), 1–10.

Thomson, S. B. (2010). *Sample size and grounded theory*. Academic Press.

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *The processes of technological innovation. Issues in organization and management series*. Lexington Books. Available at [Http://www. Amazon. com/Processes-Technological-Innovation-Organization/Management/dp/0669203483](http://www.amazon.com/Processes-Technological-Innovation-Organization/Management/dp/0669203483)

Trigueros-Preciado, S., Pérez-González, D., & Solana-González, P. (2013). Cloud computing in industrial SMEs: Identification of the barriers to its adoption and effects of its application. *Electronic Markets*, 23(2), 105–114. doi:10.1007/12525-012-0120-4

Tsai, M.-C., Lee, W., & Wu, H.-C. (2010). Determinants of RFID adoption intention: Evidence from Taiwanese retail chains. *Information & Management*, 47(5), 255–261. doi:10.1016/j.im.2010.05.001

Venkatesh, V., & Brown, S. A. (2013). Research Essay Bridging The Qualitative – Quantitative Divide. *Guidelines For Conducting Mixed Methods, X(X)*, 1–34.

Vouk, M. a. (2008). Cloud computing: Issues, research and implementations. *ITI2008 - 30th International Conference on Information Technology Interfaces*, 235–246. 10.1109/ITI.2008.4588381

Walterbusch, M., Martens, B., & Teuteberg, F. (2013). Evaluating cloud computing services from a total cost of ownership perspective. *Management Research Review*, 36(6), 613–638. doi:10.1108/01409171311325769

Wang, H. (2010). Privacy-preserving data sharing in cloud computing. *Journal of Computer Science and Technology*, 25(3), 401–414. doi:10.1007/11390-010-9333-1

Wang, Y.-M., Wang, Y.-S., & Yang, Y.-F. (2010). Understanding the determinants of RFID adoption in the manufacturing industry. *Technological Forecasting and Social Change*, 77(5), 803–815. doi:10.1016/j.techfore.2010.03.006

- Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & Stößer, J. (2009). Cloud Computing – A Classification, Business Models, and Research Directions. *Business & Information Systems Engineering*, 1(5), 391–399. doi:10.1007/12599-009-0071-2
- Wu, W.-W. (2011). Mining significant factors affecting the adoption of SaaS using the rough set approach. *Journal of Systems and Software*, 84(3), 435–441. doi:10.1016/j.jss.2010.11.890
- Wu, W.-W., Lan, L. W., & Lee, Y.-T. (2011). Exploring decisive factors affecting an organization's SaaS adoption: A case study. *International Journal of Information Management*, 31(6), 556–563. doi:10.1016/j.ijinfomgt.2011.02.007
- Wu, Y., Cegielski, C. G., Hazen, B. T., & Hall, D. J. (2013). Cloud computing in support of supply chain information system infrastructure: Understanding when to go to the cloud. *The Journal of Supply Chain Management*, 49(3), 25–41. doi:10.1111/j.1745-493x.2012.03287.x
- Xu, J., & Quaddus, M. (2012). Examining a model of knowledge management systems adoption and diffusion: A Partial Least Square approach. *Knowledge-Based Systems*, 27, 18–28. doi:10.1016/j.knosys.2011.10.003
- Yang, H., Huff, S. L., & Tate, M. (2013). Managing the Cloud for Information Systems Agility. In A. Bento & A. K. Aggarwal (Eds.), *Cloud Computing Service and Deployment Models: Layers and Management* (pp. 70–93). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-2187-9.ch004
- Yang, H., & Tate, M. (2012). A Descriptive Literature Review and Classification of Cloud Computing Research. *Communications of the Association for Information Systems*, 31(2), 35–60.
- Zhu, K. (2004). The Complementarity of Information Technology Infrastructure and E-Commerce Capability: A Resource-Based Assessment of Their Business Value. *Journal of Management Information Systems*, 21(1), 167–202. doi:10.1080/07421222.2004.11045794

Zhu, K., Dong, S., Xu, S. X., & Kraemer, K. L. (2006). Innovation diffusion in global contexts: Determinants of post-adoption digital transformation of European companies. *European Journal of Information Systems*, 15(6), 601–616. doi:10.1057/palgrave.ejis.3000650

Zhu, K., Kraemer, K., & Xu, S. (2003). Electronic business adoption by European firms: A cross-country assessment of the facilitators and inhibitors. *European Journal of Information Systems*, 12(4), 251–268. doi:10.1057/palgrave.ejis.3000475

Zhu, K., & Kraemer, K. L. (2005). Post-adoption variations in usage and value of e-business by organizations: Cross-country evidence from the retail industry. *Information Systems Research*, 16(1), 61–84. doi:10.1287/isre.1050.0045

Zhu, K., Kraemer, K. L., & Xu, S. (2006). The process of innovation assimilation by firms in different countries: A technology diffusion perspective on e-business. *Management Science*, 52(10), 1557–1576. doi:10.1287/mnsc.1050.0487

Zhu, Y., Li, Y., Wang, W., & Chen, J. (2010). What leads to post-implementation success of ERP? An empirical study of the Chinese retail industry. *International Journal of Information Management*, 30(3), 265–276. doi:10.1016/j.ijinfomgt.2009.09.007

KEY TERMS AND DEFINITIONS

Cloud Computing: A model that provides ubiquitous, convenient and on-demand access to a shared network and a set of configurable IT resources (such as networks, servers, storage, applications, and services) that can be provisioned and released with minimal administration.

Diffusion of Innovations Theory (DOI): A model organization's adoption of a technology depends on the characteristics of that technology defined by five attributes: relative advantage, compatibility, complexity, observability, and trialability.

IaaS (Infrastructure as a Service): Provides you with IT infrastructure, virtual or physical machines (quite often) and other resources such as file servers, data storage, firewalls, load balancers, IP addresses, virtual local area networks, etc.

PaaS (Platform as a Service): Provides you with computer platforms that generally include the operating system, programming the language execution environment, database, web server, etc.

SaaS (Software as a Service): Provides an access to the software application often referred to as on-demand software. You don't have to worry about the installation, configuration and operation of the application. The service provider will do it for you. You just have to pay (usually a monthly subscription depending on the number of workstations) and use it through your client interface (desktop or laptop, tablet).

Technology Organization Environment (TOE): Identify technology characteristics, organizational readiness of the company and environmental conditions as key factors in technology adoption.

Section 4

Information Security Governance in Large Organizations

Chapter 7

Information Security Governance Practices and Commitments in Organizations

ABSTRACT

Despite the existence of referential and standards of the security governance, the research literature remains limited regarding the practices of organizations and, on the other hand, the lack of a strategy and practical model to follow in adopting an effective information security governance. This chapter aims to explore the engagement processes and the practices of organizations involved in a strategy of information security governance. The statistical and econometric analysis of data from a survey of 1000 participants (with a participation rate of 83.67%) from large and medium companies belonging to various industries such as retail/wholesale, banking, services, telecom, private and governmental organizations provides a record of current practices in information security governance. The findings allowed the authors to propose a practical framework to evaluate the information security governance in organizations.

DOI: 10.4018/978-1-5225-7826-0.ch007

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

The threat to technology-based information assets is greater today than in the past (Maleh, Sahid, Ezzati, & Belaisaoui, 2018). The evolution of technology has also reflected in the tools and methods used by those attempting to gain unauthorized access to the data or disrupt business processes (L. Goodhue & Straub, 1991). Attacks are inevitable, whatever the organization (“Information Security Governance,” 2006). However, the degree of sophistication and persistence of these attacks depends on the attractiveness of this organization as a target (F. Rockart & D. Crescenzi, 1984), mainly regarding its role and assets. Today, the threats posed by some misguided individuals have been replaced by international organized criminal groups highly specialized or by foreign states that have the skills, personnel, and tools necessary to conduct secret and sophisticated cyber espionage attacks. These attacks are not only targeted at government entities. In recent years, several large companies have infiltrated, and their data have been “consulted” for several years without their knowledge. In fact, improving cybersecurity has emerged as one of the top IT priorities across all business lines. So, while companies (von Solms & van Niekerk, 2013; Bowen, Chew, & Hash, 2007)

Areas such as the aerospace industry and strategic resources can be ideal targets for cyber espionage by nation-states, others managing financial assets or large-scale credit card information are equally attractive to international criminal groups (Posthumus & von Solms, 2004; Humphreys, 2008).

These malicious actors no longer content themselves with thwarting the means of technical protection. Instead, they survey and exploit a variety of weaknesses detected in the targeted environment (Galliers & Leidner, 2014). These shortcomings are not only technological but also result from failures in protection procedures or gaps in vulnerability management practices. The best technology in the world, if misused will not provide an adequate defense against such threats (von Solms & van Niekerk, 2013).

Ensuring the information system IS security in a large organization is a real challenge (Sohrabi Safa, Von Solms, & Furnell, 2016). Only a good governance can reassure the general management, customers and partners, shareholders and ultimately the public at large (Mark Duffield, 2014).

The problem is that the security governance framework is designed to guide organizations in their IS security governance strategy but does not define the practical framework for the engagement in this strategy.

To address these concerns, some best practices and international standards (NIST, ISACA, ISO 27000 suite...) now includes chapters on security governance. The first reports or articles in academic journals that evoke the governance of information security date back to the early 2000s.

The proposed referential and best practices designed to guide organizations in their IT security governance strategy. However, does not define the practical framework to implement or to measure the organization engagement in term of IT security governance.

In this paper, we will study the practices and commitments of organizations in IS security governance. A survey of 836 medium and large companies at the international level (USA, UK, France, Morocco, China, Russia, etc.) was set up to define the best practices of these organizations regarding information security governance ISG. This study allowed us to propose a practical framework to evaluate the organization in their maturity state and to improve their level of information security governance according to their needs and resources.

The chapter is structured as follows. Section 2 presents the previous work on information security governance proposed in the literature. Section 3 describes the research methodology. The Section 4 presents the survey carried out among 836 medium and large international companies and gave a faithful picture of their practices in information security governance through statistical analysis. Then, we analyze and discusses the results of this research. Section 5 describes the proposed capability maturity framework for information security governance. Finally, Section 6 presents the conclusion of this work.

LITERATURE REVIEW AND BACKGROUND

In management sciences, several authors put forward the responsibilities and roles of management and in particular of the general management. Thereby, Straub and Welke (1998) argued that the security risk for IT can be reduced when managers are aware of the extent of existing controls and implement the most efficient controls based on the identified risks. Williams (2001) then the president of ISACA and co-founder of the IT Governance Institute recalled that directors of organizations are responsible for protecting shareholder value and that this responsibility applies to valued information assets. Rockart and Crescenzi (1984) and Markus (1983), as well as Knapp, Morris, Marshall, and Byrd (2009) confirmed that security must take into account at the general management level of the organization.

Several authors have studied the added value, the strategic or competitive advantage provided by the implementation of an information security governance. In this sense, Schou and Shoemaker (2006) found that to provide a greater benefit to the organization, the information security governance can eventually coordinate with strategic approaches to economic intelligence, social responsibility or communication. Huang, Lee, and Kao (2006) relied on a balanced dashboard to establish performance indicators for information security management in organizations and to strengthen the link between these indicators and the institutional strategy. Williams (2007) outlined the roles of management and the board of directors in the area of information security. Dhillon, Tejay, and Hong (2007) presented the results of an empirical study to understand the dimensions of IS security governance better. Kraemer, Carayon, and Clem (2009) showed that human and organizational factors play a significant role in the development of vulnerabilities related to IS and suggest a multilevel approach to improve the security performance. Johnston and Hale (2009) examined the strategic aspects of information security and try to assess the added value to the organization through the security governance approach. The authors proposed an information security roadmap based on a survey conducted among security professionals and suggest programs for its implementation. For (Kryukov & Strauss, 2009), the added value and the performance are two crucial elements of information security governance.

In his book on information security governance, (Brotby, 2009) devoted several chapters to the roles and responsibilities of managers, to the strategic measures and benefits of the approach, to the development and the implementation of a strategy for information security governance and incident management. Klaic (2010) discusses the need to define a level of governance in the organization and clarifies the link between that level and security programs.

Da Veiga and Eloff (2010) provided a framework to develop a culture of information security within an organization and illustrating how to use it. An empirical study conducted to validate the proposed culture of information security. Whitman (2011) proposed in their article value to the Executive by first defining governance as it applied to the information security and the exploration of three specific governance issues. The first inspected how government can be used to the critical aspect of planning for both formal operations and contingency operations. The next issue describes the need for programs measurement and how it can develop an information security assessment and a continuous improvement.

Finally, aspects of effective communication between and among the general security and information managers presented. Williams, Hardy, and Holgate (2013) illustrate the malleability and heterogeneity of information security governance ISG across different organizations involving intra- and inter-organizational trust mechanisms. They identify the need to reframe ISG, adopting the new label information to protecting governance (IPG), to present a more multifaceted vision of the information protection integrating a vast range of technical and social aspects that constitute and are constituted by governance arrangements. The objective of Yaokumah (2014) is to assess the levels of implementation of information security governance (ISG) in the main sectors of the Ghanaian industry. The purpose is to compare the implementation of the ISG of the inter-industry sector and to identify areas that may require improvement.

In their study, Horne, Ahmad and Maynard (2015) argue for a paradigm shift from internal information protection across the organization with a strategic vision that considers the inter-organizational level. In their paper, Soomro, Shah and Ahmed (2016) by using a systematic approach to the literature review, they synthesized the research on management roles in information security to explore management activities and to improve the information security management. They found that many management activities, in particular, the development and implementation of information security policy, awareness raising, compliance training, development of an efficient commercial information architecture, IT infrastructure management, IT alignment, business and human resource management have a significant impact on the quality of information security governance. They argue that a more holistic approach to information security is needed and suggest how managers can play a useful role in information security.

In the recent work, Carcary, Renaud, McLaughlin and O'Brien (2016) proposed a maturity framework that helps organizations to assess their ISG maturity and identify problems. It addresses the technical, procedural and human aspects of information security and provides guidelines for the implementation of information security management and related business processes.

RESEARCH METHODOLOGY

Our literature review suggests that information security has gradually moved from an operational to a strategic dimension. Past contributions have proposed

various models for information security governance, discussed the role of management and the added value of this approach. But it appears that the issue of the involvement of organizations in the information security governance process has not yet been studied.

Moreover, within the academic community, difficulties are regularly reported by security researchers, both in the development of theories (Dlamini, Eloff, & Eloff, 2009) and in empirical research (low participation rates in studies attest to this); apart from a few case studies, surveys identifying the detailed practices of a significant sample of organizations in information security governance are rare. It seems to us that a state of current organizational practices, based on new data, would update knowledge in this area of research. Therefore, we propose to answer two questions here:

- What are the factors that determine the commitment of organizations to information security governance?
- How to define a conceptual maturity framework based on best practices and commitments in organizations?

Data Collect

Our data are collected from large and medium companies on an international scale. There are several justifications for this choice. Governance first implemented by large firms, Waddock and Graves (1997) demonstrated that organizations with significant financial resources can invest more in strategic activities (Archibugi & Michie, 1995). Cohen (2006) stated that organizations must consider the security dimension in their strategy when they operating in a competitive environment, which is often the case for large enterprises. Moreover, Small and medium-sized enterprises SMEs has always shown an overall lack of security awareness (Mitchell, Marcella, & Baxter, 1999). They faced more serious problems than those encountered by large companies regarding security difficulties and a realistic assessment of the risks involved (Siponen & Willison, 2009; L. Goodhue & Straub, 1991; Peltier, 2013).

Hong, Chi, Chao, and Tang (2006) investigated the dominant factors for an organization to build an information security policy ISP, and whether an ISP may elevate an organization's security level in Taiwan. De Haes and Van Grembergen (2006) interpreted some important existing practices and models in the IT governance field and derives open research questions and some research suggestions from it. They form the basis of the pilot case research in Belgian organizations. Lomas (2010) argues that by integrating

ISO 27001 the international information security standard in co-occurrence with the ISO 15489 document management standard, holistic information governance strategies will provide a responsive response to changes in UK context. Bahl and Wali (2014) examined, as a case, the perceptions of the ISP's (Service Provider) in India regarding information security governance and its impact on the security service quality. Ula, Ismail, and Sidek (2011) proposed an initial framework for governing the information security in the banking system. The framework classified into three levels: tactical level, strategic level, operational level and technical level. This proposed framework implemented in a banking environment. Mohamed and Singh (2012) proposed a conceptual framework that examines information technology governance effectiveness, its determinants, and its impacts on private organizations.

Hung, Hwang and Liu (2013) proposed an ISG maturity model to search for relevant maturity characteristics of ISG. According to the information security assessment and maturity assessment tool, this study found that schools with a little maturity rate occupied 59.8%, 31.7% average and 8, 5%. With correlation analysis, this study concludes that 33 elements have a significant correlation with ISG maturity. With ANOVA, Post hoc scoping test, and ANOVA multiple comparative difference, this study finds that there are significant differences between the ISG maturity components. This study also finds that the maturity of schools is basic. They can improve their information security governance maturity according to this model.

Lunardi, Becker, Maçada and Dolci (2014) attempted to study and measure the improvement in the financial performance of firms that have adopted an IT management and governance strategies through pre- and post-adoption measures. They found that the organizational activities of improved IT governance practices boost their performance compared to the control group, particularly about profitability. They also concluded that the impact of adopting an IT management and governance mechanisms on financial performance was more pronounced in the year following the adoption than in the year in which they took. Adéle da Veiga and Martins (2015) discussed through a case study of an international financial institution in which ISCA conducted at four intervals over a period of eight years in twelve countries. Multivariate and comparative analyses performed to determine whether the culture of information security has improved from one evaluation to another depending on the development actions implemented. One of the primary measures performed was training and awareness-raising on the critical dimensions identified by ISCA. The culture of information security

has improved from one evaluation to another, with the most positive results in the fourth assessment.

Dhillon, Syed and Pedron (2016) used Hall's theory of cultural message flows (1959) to evaluate disturbances in the security culture following a merger. They conducted an exhaustive case study of a company in the telecom sector. The data were collected during the merger, allowing us to evaluate the changing structures in real time. The results of this analysis help researchers and practitioners to theorize on the formulation of security culture during a merger. On the practical side, decision-makers will find this analysis useful for engaging in strategic security planning.

Eroğlu and Çakmak (2016) measured information systems regarding information security and risk. On the other hand, it also aims to describe the potential effects of evaluation techniques and tools for state organizations to manage their critical assets. The information systems of one of the major healthcare organizations in Turkey have evaluated through an international assessment tool adapted to Turkish specificities and conditions in certain parts of the legal regulations. The results obtained through an evaluation tool provide the current level of maturity of the organization and point out areas that should improve the security of information systems and essential components such as risks, processes, people, IT dependence and technology.

Demography Characteristics

The target organizations belong to almost all sectors of activity: telecommunications and information technology, construction, transport, industry, commerce, services, and finance. This sectoral breakdown is in line with the International Standard Industrial Classification of All Economic Activities (Revision 4) (Nations, 2008) commonly used in community surveys.

The questionnaire was carried out in several stages. A first version has been developed to take into account the different theoretical assumptions. This first version has been tested with security managers and consultants. This pre-test allowed rephrasing certain questions to improve the comprehension of the questionnaire and to improve the quality of the given answers. In the end, the questionnaire consists of 45 questions divided into five topics: knowledge of the governance of information security and its strategic issues, its implementation conditions, its organization, its maturity level, and economic characteristics of the responding organizations. The questionnaire

was written in the three most widely spoken languages in the organizations, namely English, French, and Spanish.

Data collection was conducted during the last quarter of 2016. It took place in two steps. Firstly, 1000 questionnaires were transmitted by email to participants, using Google's facilities, giving 890 responses. 54 questionnaires were not considered mainly for confidential reasons (65%), informal organization or outsourcing (20%), contact not interested (15%). Finally, 836 final questionnaires examined for data analysis. A response rate of 83.6%. Table 1 shows the demographics of participants in a concise form.

Measurement Survey Model

In this study, we confronted a qualitative data to modeling the organization engagement or not in an approach to information security governance. We note the lack of continuity in the modalities of the variable explained. We have chosen to implement a multivariate analysis. This choice finds its motivation in the fact that we will be able to isolate the influence of the variation of a characteristic, to the exclusion of any other factor (analysis other things being equal) on the probability of engagement or not in a IS security governance. Engaging or not in such approach is a binary variable that takes the value 1 for a positive response and the value 0 for a negative response. This characteristic of the explained variable requires the use of specific methods, in this case, simple Logit and Probit dichotomous models.

We consider the sample of our population of 836 organizations of indices ($i = 1, \dots, n$, where $n = 836$). For each organization, it observed whether an individual event had taken place and:

- ($Y_i = 0$) if the organization i engages in a governance approach to information security.
- ($Y_i = 1$) if the organization i do not engage in such an approach.

We note here the choice of the coding (0,1) which traditionally retained for dichotomous models. Indeed, it allows defining the probability of occurrence of the event as the expectation of the variable y_i , since:

Dichotomous models admit for variable explained that the probability of occurrence of this event is conditional on the exogenous variables. The model takes the following form:

Information Security Governance Practices and Commitments in Organizations

Table 1. Participants' demographics

Variables		Frequency	Percent
Gender	Male	480	57,42%
	Female	356	42,58%
Age (years)	21–30	185	22,13%
	31–40	290	34,69%
	41–50	240	28,71%
	51 and above	121	14,47%
Position	Top manager personnel	99	11,84%
	IT Manager/Risk Manager/Security Officer	266	31,82%
	Security Consultant/Engineer/Analyst	471	56,34%
Number of participants	Retail/wholesale	162	19,38%
	TelComs/IT	257	30,74%
	Financial Services	183	21,89%
	Education	95	11,36%
	Government	139	16,63%
Size of the Company (# of Employees)	Fewer than 500	263	31,46%
	500–999	227	27,15%
	1,000–4,999	155	18,54%
	5,000–10,000	118	14,11%
	More than 10,000	73	8,73%
Geography	North-America	116	13,88%
	Asia-Oceania	156	18,66%
	Europe/Middle-East/Africa	343	41,03%
	Central and South America	114	13,64%
	Global	107	12,80%
Evolution of Turnover and Revenue of the Company in \$	Less than 1 million	216	25,84%
	million 1 million–5	243	29,07%
	6 million–10	166	19,86%
	10- 50	93	11,12%
	50-100	65	7,78%
	100-500	38	4,55%
	More than 500 million	15	1,79%

$$p_i = \text{Prob}(y_i = 1 | x_i) = F(x_i\beta)$$

where the function $F(\cdot)$ Denotes a distribution function, x_i denotes the explanatory variables and β the vector of the parameters to be estimated.

If y_i^* is a latent (unobservable) variable that depends on the explanatory variables x_i , the vector of the parameters to be determined (noted β) and the error term (noted ϵ_i), and then the probabilistic decision rule is written:

$$\text{Prob}(y_i = 1) = \text{Prob}(y_i^* > 0) = 1 - F(-\beta x_i) = F(\beta x_i)$$

$$\text{Prob}(y_i = 0) = \text{Prob}(y_i^* \leq 0) = F(-\beta x_i) = 1 - F(\beta x_i)$$

where β is the vector of the estimated coefficients and $F(\cdot)$ is the distribution function.

The distribution function $F(\cdot)$ Can be of two types: either a logistic law (Logit model) or a regular centered reduced law (Probit model). The results obtained from the Logit and Probit models are relatively similar (Morimune, 1979; Davidson & MacKinnon, 1984). For our estimates, we will retain a Logit model where the estimation of the parameters of the model is carried out by the method of maximum likelihood.

Since the analysis population is medium in size (836 organizations), the number of explanatory variables introduced into our models should be limited. To remove this constraint, we have aggregated the modalities of individual variables. To take advantage of the richness of the questionnaire, we have created variables that synthesize the available information and make several estimates where all available information introduced alternately. More precisely, the sectors of activity grouped into three areas: industry, service, finance (variables IND, SRV and FINA). The results obtained with this specification show that membership in the banking sector does not affect the probability of engaging in information security governance.

To take into account the change in turnover for each organization, we will focus on the impact of a growing turnover variable (TURNOVER). So that's the way in which the variables constructed does not affect our estimates, certain characteristics are taken into account using different variables.

Thus, knowledge of the environment and structures engaged in a security governance approach will be taken into account in three ways:

- Using the number of structures involved in a security governance strategy that the organization knows, between 0 and 3 (variable NB_INVOLVED);
- Using a variable knowing other organizations involved in a security governance strategy, implemented locally, regionally or internationally (variable INVOLVED);
- Using a variable to identify competitors involved in a security governance approach (variable COMPETITORS);
- Using a variable: Identifying organizations whose promoting the security governance approach (variable ORGANIZATION).

To consider the benefits, obstacles and priority areas taken from an approach to information security governance, we will introduce each benefit, barrier and focus area in turn. We also constructed three variables that take into account the number of benefits derived from an information security governance approach (NB_BENEF), the number of obstacles and challenges encountered (NB_CHALL) and the number of priority areas (NB_PRIORITY). The set of variables introduced in our model presented in Appendix 1 (Table 3).

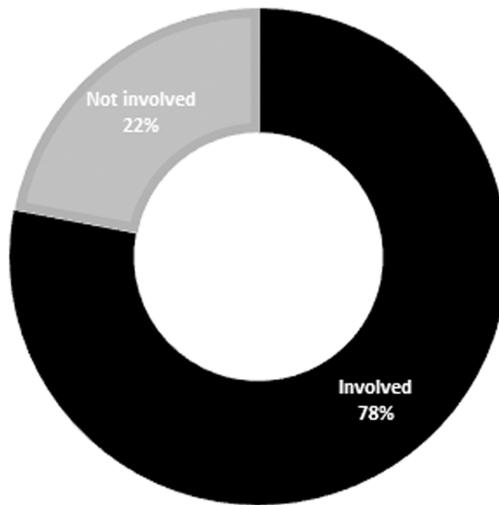
SURVEY RESULTS

This section shows the detailed practices of organizations interviewed in the area of information security governance using descriptive statistics, thus answering our second research question.

IT Security Governance Knowledge

The survey reveals that 78% of organizations are familiar with practices of information security governance, mainly through the Internet, vocational training and technology watch. As shown in Figure 1, 75% of these organizations are involved in an approach to information security governance. 80% of organizations are aware of other organizations involved in information security governance, of which 34% are clients, 59% are suppliers, and 41% are competitors. Eighty of these organizations (78%) are involved in the governance of information security.

Figure 1. Involvement of organizations in governance approach to the security of the information system



Conditions for Implementing Information Security Governance

Before embarking on an approach to information security governance, practicing organizations took stock of actions already carried out internally (81%) as well as possible envisaged measures (87%), knowledge of standards and certifications (80%). Collected information from specialized security agencies and organizations (73%), evaluated of security budget and costs (75%) and reviewed actions by other organizations (39%). These results illustrated in Figure 2.

On average, 5 persons per organization assigned to the ISG process, including 2 managers, 2 members of the IT team, 1 external consultant. Almost one out of every two organizations (59%) has a budget dedicated to information security. The implementation of information security governance is described and valued by 38% of organizations in their activity report, by 27% on their website, by 63% in their internal documents (intranet, Procedures, IT charts), Nowhere for 23% of them. Similarly, 71% of the organizations have plans to communicate their commitments internally, 22% to the outside and 29% have not talked at all about these commitments.

Strategic Issues in Information Security Governance

In organizations that practice information security governance, its implementation is primarily the result of the need to satisfy customers (79%). It is intended to satisfy shareholders and management (48%), employees (40%), legislation in force (36%), suppliers (17%), local authorities or non-governmental organizations (12%). 95% of organizations believe they can gain a competitive advantage (very significant or significant benefits) from information security governance, and 75% are committed to the process. Among the benefits of an approach to information security governance, which are considered very important, organizations mainly focus on improving security procedures and strategies (73%). Quality improvement of information protection (65), compliance with legislation (35%), and Trust for partners (31%). These results are illustrated in Figure 2 below.

Conversely, 93% of organizations interviewed perceive difficulties (very significant or significant obstacles) in the implementation of information security governance, yet 74% are involved in the process. Examination of the obstacles considered very important by the organizations shows, in descending order of citation. The lack of time (27%), the lack of internal talent (24%), the lack of top management interest (19), the cost of implementation (17%). These results illustrated in Figure 3. Within organizations practicing the governance of information security, the responsibility for this process is entrusted to an IS/IT (CIO) for 53% of them, a risk manager for 14% a chief executive officer (CEO) for 13%. A quality/compliance manager for 12%, and a CISO (Chief Information Security Officer) in only 8% of cases.

Figure 2. Key benefits of information security governance

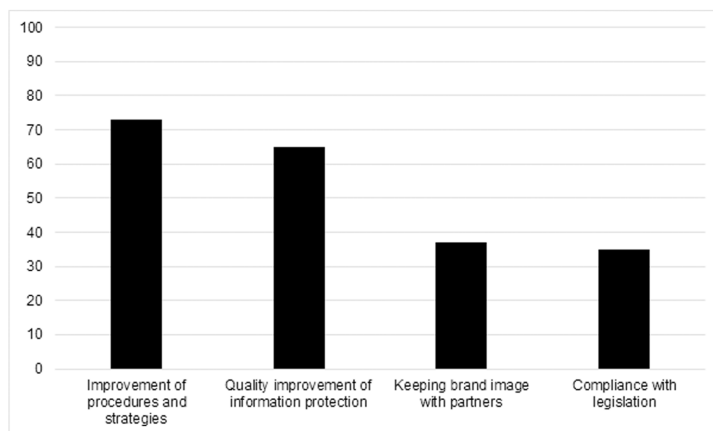
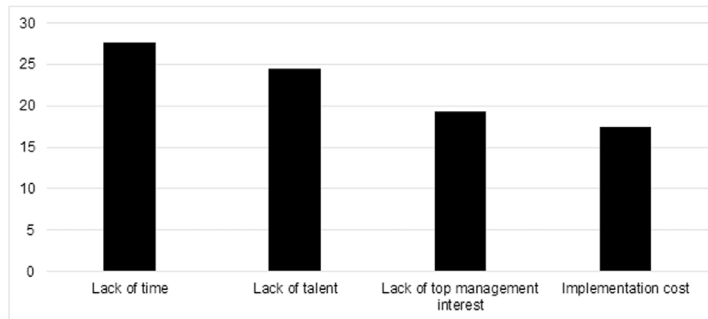


Figure 3. Key obstacles to the implementation of information security governance



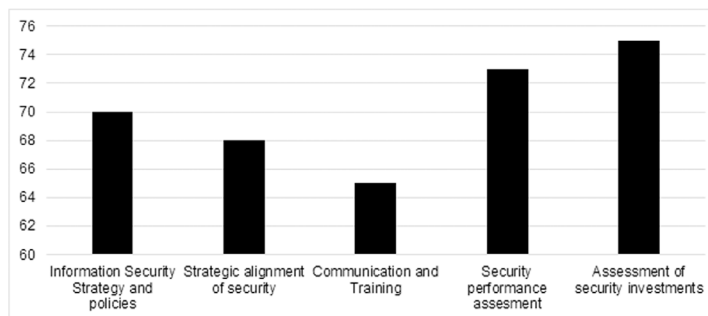
IT Security Governance Strategy and Metrics

According to the responding organizations, 70% of the organizations confirm that the definition of a strategy and policy plays the main role in adopting a governance approach to information security. Strategic alignment of security (68%), communication and training (63%), evaluation of performance by monitoring security indicators (73%), of value through optimization of security investments (75%). These results are illustrated in Figure 4.

IT Service and Asset Security Management

Among the organizations practicing the governance of information security, 66% set measurable targets, such as reducing security incidents, reducing operational risk, implementing incidents management tools and procedures Security, etc. In terms of the definition of information security classes and data classification, 66% of the organizations take no interest in this axis.

Figure 4. Information security governance: Strategy and metrics



78% of the organizations confirm the mastery of the technical architecture of their IS security, and 83% implement measures to manage their IT assets (servers, networks, storage devices, printers, and smartphones). 68% have a management and a return on investment concerning the hard and soft resources deployed for the security of the IS of the organization. 66% have access to management tools and policies that enable them to identify and trace the various SI access operations, including granting, denying, and revoking access privileges. Figure 5 below illustrates the results.

Vulnerability and Risk Management

According to the responding organizations, the priority areas (or values) of an information security governance approach is vulnerability and risk management. In terms of the security threats profile, 70% of organizations are adopting a process to gather information on computer security threats and vulnerabilities to better understand the landscape of the IT security threat in which the organization operates. 68% assess safety risks and quantify their probability and potential impact. 65% adopts a process of prioritizing risks according to its impact on the organization. 73% adopt tools and processes for risk monitoring and management and information security control options. The results are illustrated in Figure 6.

Information Security Compliance, Control, and Verification

To avoid any infringement of the intellectual property, legal, regulatory and contractual provisions and security requirements of the organization. The organization must adopt an approach to Compliance. Verification is focused on the processes and activities related to how an organization checks, and

Figure 5. IT service and asset security management practices in organisations

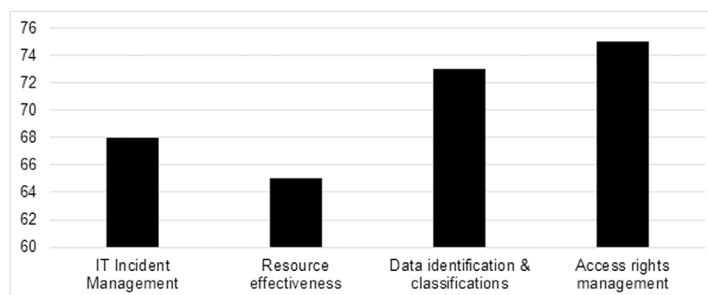
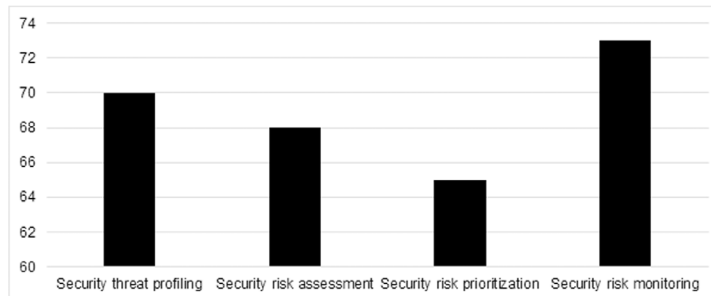


Figure 6. Vulnerability and risk management practices in organisations



tests artifacts produced throughout software development. This typically includes quality assurance work such as testing, but it can also include other review and evaluation activities.

Among the organizations practicing the governance of information security, 80% adopted compliance repositories such as ISO 2700x and PCI DSS, 70% have conducted at least one IT security audit in the last 3 years. 60% have developed action plans, either current or future, within the framework of the governance of information security, such as the implementation of a business continuity plan, staff training, Network redundancy, data centralization, server virtualization, improved traceability, etc.

Organizational Maturity of Information Security Governance

In total, 51% of the organizations interviewed confirm that the governance of information security is indispensable 40% consider it necessary, 6%

Figure 7. Security compliance, control and verification practices in organizations



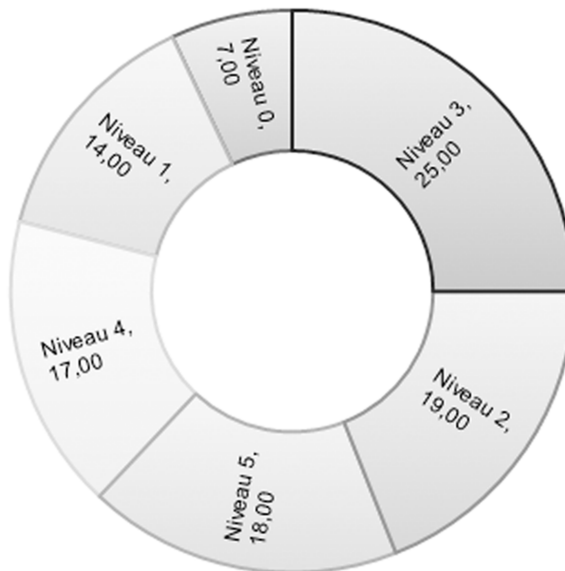
unhelpful and 3% useless. 87% of those surveyed perceive governance of information security as a significant value for the organization; 78% of these organizations are engaged in an information security governance approach. By analyzing the maturity of organizations in the governance of information security according to a typology proposed by the (“Information Security Governance,” 2006), it appears that:

- For 7% no procedure is applied. The organization does not recognize any need for information security. No obligation or liability is established. That corresponds to the basic level (level 0);
- 14% of procedures exist but remain disorganized. IT risks are assessed ad hoc per project. The organization recognizes the need to secure its information resources but reactively. Responsibilities are informal. That corresponds to level 1;
- For 19% the procedures follow a defined model. IT risks are considered significant. Security policies are developed. The report is incomplete or inadequate. That corresponds to level 2;
- For 25% the procedures are formalized, documented and communicated by an organizational policy. The report remains focused on IT rather than on the organization. That corresponds to level 3;
- For 17% the procedures are monitored and measured. A senior manager provides the security function. Responsibilities are applied. The report is linked to the objectives of the organization. That corresponds to level 4;
- For 18%, procedures, safety technologies, and contingency plans are integrated into the organization’s activity, optimized and automated. The report makes it possible to anticipate the risks. That corresponds to level 5.

These results are illustrated in Figure 8.

The projects portfolio of information security governance does not include any projects for 23% of organizations surveyed. Projects are envisaged for 43% of them (on average two projects per organization); Projects are in progress for 67% of the organizations (on average three projects per organization), and projects have closed during the last three years for 43% of them (on average four projects per organization). 87% of organizations that have embarked on an information security governance approach to report organizational changes: recruitment of external management profiles (31%). Changes in

Figure 8. Information security maturity according to the IT Governance Institute (2006)



internal business for 59% (for example, changes in the technical profiles Specialization), implementation of specific training for 63%.

DISCUSSION AND INTERPRETATION

To answer our first research question, we present the different determinants of the organizational engagement process in an information security governance approach, using the Logit model specifications as described in the research methodology section. We define several models to introduce the determinant variables to ensure the quality of the effects obtained. Table 4 (Appendix 2) describes the results of the 5 models used. Model 1 highlights the positive impact of the expected benefits of an information security governance approach on the likelihood of adopting it. It is also noted that the number of organizations known to have adopted an information security governance approach has a positive effect on the probability of adopting such an approach. On the other hand, the economic characteristics of the organization (its sector of activity, the growth of its turnover, membership of a group) do not affect results.

To refine this last result, we have introduced successively different obstacles encountered by the organizations. We note that only 2 obstacles have a significant effect: the difficulty of translating concepts into concrete actions is a brake on the adoption of information security governance (model 2); the low interest of top management for issues related to information security also has a negative impact (model 3). The simultaneous consideration of these two obstacles confirms only the negative effect of the difficulty in translating the concepts into concrete actions (model 4).

The set of models 1 to 5 shows that the number of values shared by the organization under the governance of information security policy does not affect its adoption. When the values considered important by the organization are taken into account successively, this result persists.

A detailed analysis of the impact of the organization's environment (knowing an organization with an information security governance approach, recognizing an organization that seeks to promote it) shows that the organization's environment has a positive effect on the probability of adopting such an approach, regardless of how this dimension is taken into consideration. Generally speaking, on models 4 and 5, the effects obtained in the model that could be qualified as model 1 are summarized: the growth of turnover and the number of values of the "organization do not affect. Knowledge of other competing organizations at the regional or international level has a positive effect on the adoption of governance information security (Model 5).

Given that the benefits derived from a security governance approaches have a positive effect on the probability of adopting models 1 to 5, we have successively introduced each profit considered necessary by the organization to identify the with profits having a positive impact. The variables not having a significant effect on the probability of adopting an information security governance approach have not been reported in the corresponding results in Table 4 of Appendix 2. This result shows that it is the accumulation of different benefits deemed essential that prompts organizations to embrace such an approach and not the impact of a particular benefit.

In summary, the probability of adopting an information security governance approach is positively affected by the number of benefits derived from such an approach, by the knowledge of structures involved in this process (organizations that have implemented this approach and organizations to promote it). The difficulty of translating concepts into concrete actions is the only one that adversely affects the likelihood of adopting an information security governance approach. Belonging to the industry sector, as compared to the service sector, negatively impacts this probability. Other characteristics

of the organizations (group membership, growth turnover) and their values do not affect. Figure 9 summarizes the proposals suggested by our research on the determinants of organizational engagement in information security governance.

Note that the proposed determinants of the organizational engagement process in information security governance are very close to the four determinants identified by (Venkatesh, Morris, Davis, & Davis, 2003) (Venkatesh, 2012). In their Unified Technology Adoption Unified Theory of Acceptance and Use of Technology UTAUT model, as shown in Figure 8. This model synthesizes eight previous models into four main determinants. (PE) Performance Expectancy of the governance approach (added value, benefits, and competitive advantage). (EX) Effort Expectancy deployed for its implementation (overcoming brakes, obstacles). (FC) Facilitating Conditions (knowledge of organizations likely to help the organization in its approach). (SI) Social Influence (subjective norms, image, values). The proximity of our results to this model would suggest that the commitment of organizations in the governance process could be compared to the commitment that organizations could make to innovation, in other words to the adoption of innovation.

However, all the conditions of the UTAUT model are collected in our survey. In particular, the four moderating variables (gender, age, education level, experience) that have significant influence in the model have not been

Figure 9. Proposed determinants process of the engagement in information security governance

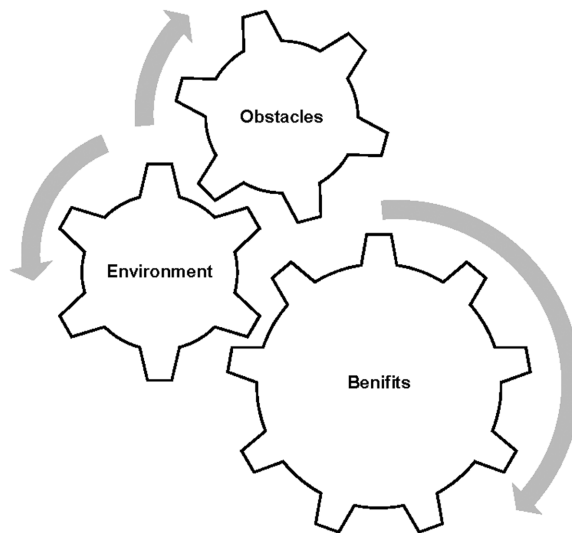
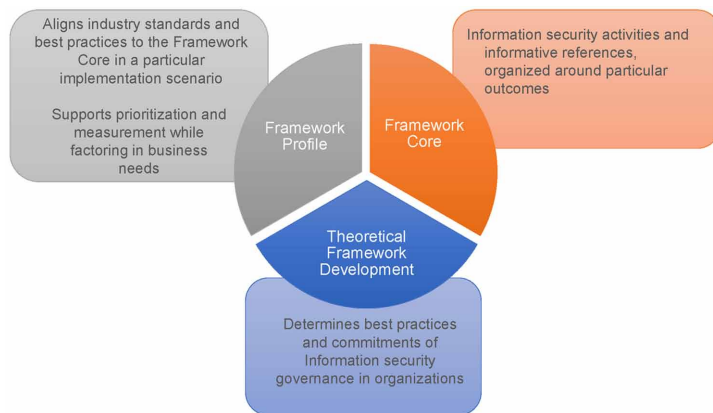


Figure 10. Unified technology adoption unified theory of acceptance and use of technology



taken into account. Aware of this limit, we can base on the survey conducted that the adoption of the unified theory of (Venkatesh et al., 2003) can be a relevant model for analyzing the phenomenon of engagement in the governance of information security.

The responses to our survey confirm that information security governance is an integral subset of IS/IT governance, as the organizations involved in both approaches are the same. The responsibility for security governance is attributed, according to the organizations, to various players ranging from the IT manager, risk manager, quality and compliance manager, chief information security officer CISO to the general manager. Within the sample studied the affiliation of the governance and the information system division concerns organizations with weak or moderately exposed information risks, where the security function is more operational than strategic and managerial aspects. The relationship between governance and risk management, audit or internal control is rather typical of organizations exposed to information risks (tertiary and quaternary sectors). The linkage of governance to the organization's general manager is preferred when information is the product of the organization, and the risk of the organization and that of the information are almost confused. It is also interesting to note another result of the survey: 31% of organizations surveyed practicing security governance did not value this approach either internally or externally, and 33% have not communicated at all about their engagements. Evidence that the governance of information security is not necessarily considered as an asset in the communication plan of the organization with its various partners and collaborators.

Given the results of the survey, it seemed interesting to test whether the perception of the stakes of the governance of the information security was the same or not, for the organizations involved in the process and for those n 'Having no practical experience. Given the distinction made in the questionnaire about the organizations involved in the governance of information security. We observe 100% similarity in the ranking of the first three profits by comparing the responses of each type of information security, Organization. The ranking then differs from only a few organizations (less than 30) for the following benefits. Regarding the perceived obstacles of the approach, we observe 100% of similarity in all the results of the classification. Therefore, the perceived strategic issues of information security governance are very similar, whether or not the organization is involved in this process.

On the practical aspect, this research provides managers a detailed information on the engagement of organizations in the information security governance. The survey suggests that knowledge of organizations engaged in or promoting the process, expected performance, effort to overcome difficulties, and sharing of positive values associated with information security governance promote the organization's involvement in this process. It also describes and updates the practices of medium and large companies of different sectors involved in the information security governance, in terms of knowledge and strategic challenges, implementation conditions, governance organization. Finally, we addressed the maturity challenge of the organizations interviewed regarding information security governance.

Based on the return of experience of this empirical study and different maturity models in the literature (ISACA, ISO 2700x), we suggest in the next part of this paper a practical IT security management and governance framework.

THE RESULTANT MATURITY FRAMEWORK

In this second part of this work, we present a conceptual maturity framework for information security governance based on best practices and commitments described in the first part. The framework is based on the fact that the pace and manner in which an organization can respond proactively to new and emerging security threats. The fundamental pillars of the proposed framework must be fluid and responsive to the changing landscape of information security; By developing their capabilities to detect, assess and respond to new and emerging

security threats, organizations can position themselves more proactively to efficiently and continuously secure information resources.

Framework Overview

We propose a conceptual maturity framework to achieve an effective information security governance approach. The path to security maturity requires a diversified range of layered endpoint protection, management and capabilities, all integrated and fully automated. The only practical and survivable defensive strategy are to move to a more mature security model that incorporate multiple layers of protective technology.

The proposed framework focuses on determining the capacity of an organization to direct oversee and monitor the actions and processes necessary to protect documented and digitised information and information systems and to ensure protection against access, unauthorized use, disclosure, disruption, alteration or destruction, and to guaranty confidentiality, integrity, availability, accessibility and usability of the data (Kenneally, Jim Curley, 2012). The framework extends the triad confidentiality, integrity and availability of commonly cited with accessibility and usability concepts. Concerning accessibility, a failure to support and understand how security can change work practices can impede how data and information are accessed, shared, and acted on in an increasingly dynamic, competitive environment. Similarly, usability is a one of a main key factor to engaging stakeholders in the business processes, independently of the availability of technology to support work practices, if the technology is difficult to interact and engage with, users might adopt other locally developed, less secure methods of access.

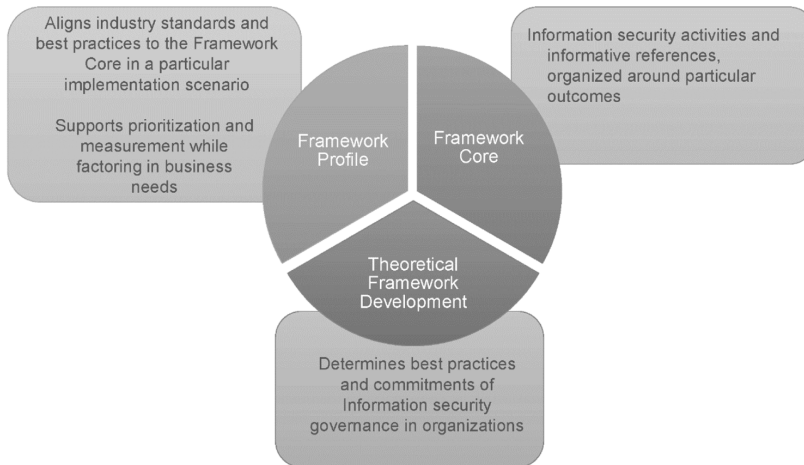
Based on the best practices and commitments defined in the first part, we propose a conceptual maturity framework for information security governance as shown in Figure 11.

Framework Core

The proposed framework classifies the information security activities across the following five high-level function categories:

- Information security strategy and governance provide the oversight structures for supporting information security governance; it implements information security strategy, policies, and controls; assigns. Define

Figure 11. The proposed conceptual framework for ISG



roles and responsibilities for ISG activities; provides communication and training; reports on ISG activities' effectiveness; and manages supplier security requirements; plans and tests the security of business continuity measures.

- Technical asset security management establishes a security architecture and implements measures to control IT component and physical infrastructure security.
- Information services, system and data management, provides security budgets, tools, and resources, and measures the resource efficiency of security investments. Defines data security classifications and provides guidance on managing access rights and data throughout its lifecycle.
- Vulnerability and risk management to control profiles security threats and assesses priorities, handles, and monitors security-related risks. a
- Information security compliance, control and verification.

The proposed information maturity framework is a comprehensive suite of proven management practices, assessment approaches and improvement strategies covering 5 governance capabilities, 21 objectives and 80 controls. As Table 2 shows, these high-level function categories are decomposed into 21 security practice objectives (SPOs).

Information Security Governance Practices and Commitments in Organizations

Table 2. The proposed framework capabilities and objectives

Governance Capabilities	Security Practice Objective	Description
Information security governance Strategy and Metrics	Information Security Strategy and policies	Develop, communicate, and support the organization’s information security objectives. Establish and maintain security policies and controls, taking into account relevant security standards, regulatory and legislative security requirements, and the organization’s security goals.
	Strategic alignment of security	From risk analysis to the actual deployment of global policy, security must be aligned with the business priorities of the company while respecting regulatory and legal constraints
	Communication and Training	Disseminate security approaches, policies, and other relevant information to develop security awareness and skills.
	People Roles and responsibilities	Document and define the responsibilities and roles for the security of employees, contractors and users, by the organization’s information security strategy
	Security performance assessment	Report on the efficiency of information security policies and activities, and the level of compliance with them.
	Assessment of security budget and investments	Provide Security related investment and budget criteria
Technical Asset Security Management	Security architecture	Build security measures into the design of IT solutions—for example, by defining coding protocols, depth of defense, the configuration of security features, and so on.
	IT component Security	Implement measures to protect all IT components, both physical and virtual, such as client computing devices, servers, networks, storage devices, printers, and smartphones.
	Physical Infrastructure Security	Establish and maintain measures to safeguard the IT physical infrastructure from harm. Threats to be addressed include extremes of temperature, malicious intent, and utility supply disruptions.
Information Service/System/Data Security Management	Incident Management	Manage security-related incidents and near-incidents. Develop and train incident response teams to identify and limit exposure, manage communications, and coordinate with regulatory bodies as appropriate.
	Resource Effectiveness	Measure “value for money” from security investments; capture feedback from stakeholders on the effectiveness of security resource management.
	Data identification and Classifications	Define information security classes, and provide guidance on protection and access control appropriate to each level.
	Access Management	Manage user access rights to information throughout its lifecycle, including granting, denying, and revoking access privileges.
	System Acquisition, Development, and Maintenance Security Policy	Ensure the management of security throughout the life cycle of Information Systems. Reduce risks related to exploiting technical vulnerabilities and applications.

continued on following page

Table 2. Continued

Governance Capabilities	Security Practice Objective	Description
Vulnerability and Risk Management	Security Threat profiling	Gather intelligence on IT security threats and vulnerabilities to better understand the IT security threat landscape within which the organization operates, including the actors, scenarios, and campaigns that might pose a threat.
	Security Risk Assessment	Identify exposures to security-related risks, and quantify their likelihood and potential impact.
	Security Risk Prioritization	Prioritize information security risks and risk-handling strategies based on residual risks and the organization's risk appetite.
	Security Monitoring	Manage the ongoing efficacy of information security risk-handling strategies and control options.
Information Security Governance Control/ Compliance/Continuity Management	Compliance Control	Identify applicable law, statutory and contractual obligations that might impact the organization. Establish security and compliance baseline and understand per-system risks.
	Security Testing and Auditing	Adopt solution for information security audit. Establish a project audit practice. Derive test cases from known security requirements
	Business continuity planning	continuity management Business continuity planning Provide stakeholders throughout the organization with security advice to assist in the analysis of incidents and to ensure that data is secure before, during, and after the execution of the business continuity plan.

Framework Maturity Profile

The bottom line on information security is that the threat environment of today is simply too dynamic. The only practical and survivable defense strategy are to move to a more mature security model that integrate multiple layers of protection technology.

We propose a mature and systematic approach to information security management and governance. Adopting a security maturity strategy requires a full range of protection, management and defensive features that must be integrated and capable of fully automated operation.

Concerning each security practice objectives SPO outlined in Table 2, the framework defines a five-level of maturity that serves as the basis for understanding an organization's ISMGO capability and provides a foundation for capability improvement planning.

Level 0 - None: No process or documentation in place.

Level 1 - Initial: Maturity is characterized by the ad hoc definition of an information security strategy, policies, and standards. Physical environment and IT component security are only locally addressed. There is no explicit consideration of budget requirements for information security activities, and no systematic management of security risks. Access rights and the security of data throughout its lifecycle are managed at best using informal procedures. Similarly, security incidents are managed on an ad hoc basis.

Level 2 – Basic: Maturity reflects the linking of a basic information security strategy to business and IT strategies and risk appetite in response to individual needs. It also involves the development and review of information security policies and standards, typically after major incidents. IT component and physical environment security guidelines are emerging. There is some consideration of security budget requirements within IT, and requirements for high-level security features are specified for major software and hardware purchases. A basic risk and vulnerability management process are established within IT according to the perceived risk. The access rights control and management depend on the solutions provided by the provider. Processes for managing the security of data throughout its lifecycle are emerging. Major security incidents are tracked and recorded within IT.

Level 3 - Defined: Maturity reflects a detailed information security strategy that's regularly aligned to business and IT strategies and risk appetite across IT and some other business units.

Information security policies and standards are developed and revised based on a defined process and regular feedback. IT and some other business units have agreed-on IT component and physical environment security measures. IT budget processes acknowledge and provide for the most important information security budget requests in IT and some other business units. The security risk-management process is proactive and jointly shared with corporate collaboration. Access rights are granted based on a formal and audited authorization process. Detailed methods for managing data security throughout its life cycle are implemented. Security incidents are handled based on the urgency to restore services, as agreed on by IT and some other business units.

Managed. Level 4: Maturity is characterized by regular, enterprise-wide improvement in the alignment of the information security strategy, policies, and standards with business and IT strategies and compliance requirements. IT component security measures on IT systems are implemented and tested enterprise-wide for threat detection and mitigation. Physical environment security is integrated with access controls and surveillance systems across the enterprise. Detailed security budget requirements are incorporated into enterprise-wide business planning and budgeting activities. A standardized security risk-management process is aligned with a firm risk-management process. Access rights are implemented and audited across the company. Data is adequately preserved throughout its life cycle, and data availability is effectively requirements. Recurring incidents are systematically addressed enterprise-wide through problem-management processes that are based on root cause analysis.

Optimized. Level 5: Maturity reflects an information security strategy that is regularly aligned with business and IT strategies and risk appetite across the business ecosystem. Information security policies and standards are periodically reviewed and revised based on input from the business ecosystem. The management of IT component security is optimized across the security framework layers. Physical access and environmental controls are regularly improved. Security budget requirements are adjusted to provide adequate funding for current and future security purposes. The security risk-management process is agile and adaptable, and tools can be used to address the business ecosystem's requirements. The access rights control and management are dynamic and can effectively deal with the organizational restructuring of acquisitions and divestitures. Processes for managing data security throughout its life cycle are continuously improved. Automated incident prediction systems are in place, and security incidents are effectively managed.

CONCLUSION

Today, protecting ourselves against IT risks through the establishment of good governance has become an essential activity to maintain the operational capacity of any organization.

This paper proposes an exploration of the determinants of organizations' involvement in the information security governance and their practices in this area. The survey conducted among 2 hundred large organizations proposes a model consisting of seven determinants of the commitment of organizations in the information security governance process: it suggests that the knowledge of organizations engaged in the governance of security Information or promotion, the performance expected and the effort deployed to encourage the commitment of organizations in the process. The responses to the questionnaire also increase awareness of current practices of information security governance implemented by organizations.

By this empirical study and the results of our survey, a framework for measuring the maturity of information security was proposed with the aim of providing a practical tool for measuring and improving governance of information security in the organization. To show the effectiveness of the proposed framework, we implemented the resultant maturity framework in a large organization. The results will be presented in the upcoming chapter.

REFERENCES

- Archibugi, D., & Michie, J. (1995). Technology and Innovation: An Introduction. *Cambridge Journal of Economics*, 19. doi:10.1093/oxfordjournals.cje.a035298
- Bowen, P., Chew, E., & Hash, J. (2007). *Information Security Guide For Government Executives Information Security Guide For Government Executives*. National Institute of Standards and Technology NIST. doi:10.6028/NIST.IR.7359
- Brotby, K. (2009). *Information Security Governance: A Practical Development and Implementation Approach*. John Wiley & Sons. doi:10.1002/9780470476017
- Cohen, F. (2006). *IT Security Governance Guidebook With Security Program Metrics*. Pennsauken, NJ: Auerbach Publishers Inc. doi:10.1201/b15999
- Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196–207. doi:10.1016/j.cose.2009.09.002

De Haes, S., & Van Grembergen, W. (2006). Information technology governance best practices in Belgian organisations. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 8. 10.1109/HICSS.2006.222

Dhillon, G., Tejay, G., & Hong, W. (2007). *Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations*. Academic Press. doi:10.1109/HICSS.2007.257

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, 28(3), 189–198. doi:10.1016/j.cose.2008.11.007

Duffield. (2014). *Global governance and the new wars: The merging of development and security*. Z. B. Ltd, Ed.

Galliers, R. D., & Leidner, D. E. (2014). Strategic information management: challenges and strategies in managing information systems. *Information Strategy*, 625. Retrieved from <http://www.worldcat.org/isbn/0750656190>

Goodhue, D., & Straub, D. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management* (Vol. 20). doi:10.1016/0378-7206(91)90024-V

Hong, K., Chi, Y., Chao, L. R., & Tang, J. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, 14(2), 104–115. doi:10.1108/09685220610655861

Huang, S., Lee, C.-L., & Kao, A.-C. (2006). Balancing performance measures for information security management: A balanced scorecard framework. *Industrial Management and Data Systems* (Vol. 106). doi:10.1108/02635570610649880

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, 13(4), 247–255. doi:10.1016/j.istr.2008.10.010

Information Security Governance. (2006). *Guidance for Boards of Directors and Executive Management*. Author.

Johnston, A., & Hale, R. (2009). Improved Security through Information Security Governance. *Commun. ACM*, 52. doi:10.1145/1435417.1435446

Klaic, A. (2010). Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies. *International Convention on Information and Communication Technology, Electronics and Microelectronics MIPRO*.

Knapp, K., Morris, R., E. Marshall, T., & Byrd, T. (2009). Information security policy: An organizational-level process model. *Computers & Security* (Vol. 28). doi:10.1016/j.cose.2009.07.001

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security* (Vol. 28). doi:10.1016/j.cose.2009.04.006

Kryukov, D., & Strauss, R. (2009). *Information security governance as key performance indicator for financial institutions* (Vol. 38). Riga Technical University. doi:10.2478/v10143-009-0014-x

Maleh, Y., Sahid, A., Ezzati, A., & Belaissaoui, M. (2018). A Capability Maturity Framework for IT Security Governance in Organizations. In A. Abraham, A. Haqiq, A. K. Muda, & N. Gandhi (Eds.), *Innovations in Bio-Inspired Computing and Applications* (pp. 221–233). Cham: Springer International Publishing. doi:10.1007/978-3-319-76354-5_20

Markus, M. (1983). Power, Politics, and MIS Implementation. *Commun. ACM* (Vol. 26). doi:10.1145/358141.358148

Michael, E., & Whitman, H. J. M. (2011). *Roadmap to Information Security: For IT and Infosec Managers*. Delmar Learning.

Mitchell, C., Marcella, R., & Baxter, G. (1999). Corporate information security management. *New Library World* (Vol. 100). doi:10.1108/03074809910285888

Mohamed, N., & Singh, J. K. a/p G. (. (2012). A conceptual framework for information technology governance effectiveness in private organizations. *Information Management & Computer Security*, 20(2), 88–106. doi:10.1108/09685221211235616

Nations, U. (2008). *International Standard Industrial Classification of All Economic Activities (Revision 4)*. New York: United Nations Publication.

Peltier, T. R. (2013). *Information Security Fundamentals* (2nd ed.). Taylor & Francis. doi:10.1201/b15573

- Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 23(8), 638–646. doi:10.1016/j.cose.2004.10.006
- Rockart, J., & Crescenzi, A. (1984). Engaging top management in information technology. *Sloan Management Review*, 25, 3–16.
- Schou, C., & Shoemaker, D. P. (2006). *Information Assurance for the Enterprise: A Roadmap to Information Security*. McGraw-Hill, Inc.
- Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), 267–270. doi:10.1016/j.im.2008.12.007
- Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 1–13. doi:10.1016/j.cose.2015.10.006
- Straub, D., & Welke, R. (1998). Coping with systems risk: Security planning models for management decision making. *Management Information Systems Quarterly*, 22(4), 441–469. Retrieved from <http://www.jstor.org/stable/249551>. doi:10.2307/249551
- Ula, M., Ismail, Z., & Sidek, Z. (2011). A Framework for the Governance of Information Security in Banking System. *Journal of Information Assurance & Cybersecurity*, 23(8), 1–12. doi:10.5171/2011.726196
- Venkatesh, V. (2012). Consumer Acceptance And Use of Information Technology. *Extending the Unified Theory*, 36(1), 157–178.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *Source: MIS Quarterly*, 27(3), 425–478. doi:10.2307/30036540
- von Solms, R., & van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security*, 38, 97–102. doi:10.1016/j.cose.2013.04.004
- Waddock, S. A., & Graves, S. B. (1997). The Corporate Social Performance-Financial Performance Link. *Strategic Management Journal*, 18(4), 303–319. doi:10.1002/(SICI)1097-0266(199704)18:4<303::AID-SMJ869>3.0.CO;2-G

Information Security Governance Practices and Commitments in Organizations

Williams, P. (2001). Information Security Governance. *Information Security Technical Report*, 6(3), 60–70. doi:10.1016/S1363-4127(01)00309-0

Williams, P. (2007). *Executive and board roles in information security*. *Network Security* (Vol. 2007). Academic Press. doi:10.1016/S1353-4858(07)70073-9

Williams, S. P., Hardy, C. A., & Holgate, J. A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electronic Markets*, 23(4), 341–354. doi:10.1007/12525-013-0137-3

APPENDIX 1

Table 3. List of variables introduced in the measurement model

Variable	Label
GEN	Gender of participants
Ag	Age (years)
NB_ORG	Number of participants organization
SIZE	Size of the Company (# of Employees)
INDUS	Belonging to industry
SERV	Belong to other sectors
FINA	Be part of a finance sector
TURNOVER	Evolution of Turnover and Revenue of the Company in \$
ORGANISME	Knowledge of an organization promoting the governance of information security
NB_BENEF	Number of benefits derived from an information security governance approach
IMAGE	Improving the image of the organization
ATTRACT	Attract new customers / employees
DIFFER	Differentiating from the competition
ESTABLISH	Building confidence
CONFORME	Compliance with legislation
CERTIF	Get certification
IMPROVE	Improve safety procedures
ENSURE	Ensure decisions and activities at risk
CONTROL	Guarantee the mastery of the computer tool
VAL	Increase the value of the organization
INCREASE	Increase predictability and reduce uncertainty in management operations

continued in following column

Table 3. Continued

Variable	Label
RESP	Do not incur civil / legal liability
RESOURCE	Optimize security resources
NB_CHALL	Number of barriers to implementing an information security governance approach
COST	Cost of Implementation
TEMPS	Lack of time
HOUSERES	Lack of in-house resources
SKILLS	Lack of in-house skills
INFO	Difficulty in finding relevant information
CHANGE	Resistance to change
MANAGEMENT	Low level of management interest
ACTIONS	Translation of the concept into concrete actions
NB_PRIORITY	Number of priority areas for engagement in a governance approach to information security
TECHNO	Safety-Related Technology Choices
ALIGN	Aligning information security with organizational strategy
RISQUE	Risk management and reduction of potential impacts to an acceptable level
RESSOURCE	Management of Information Resources
PERF	Evaluation of performance through the monitoring of safety indicators
CREAT	Creating value through optimization of security investments

APPENDIX 2

Table 4. The determinants of the adoption of information security governance (Logit model)

Variable	Model 1	Model 2	Model 3	Model 4	Model 5
Constante	-0.6983 (0.7184)	-1.0383 (0.7556)	-0.8540 (0.7376)	-0.8863 (0.7183)	-1.3922* (0.8330)
INDUS	-0.7934 (0.6134)	-0.8387 (0.6465)	-0.8684 (0.5454)	-0.9198 (0.5674)	-0.9606* (0.5735)
SERV	Référence	Référence	Référence	Référence	Référence
FINA	0.5037 (0.6239)	0.5275 (0.6538)	0.4239 (0.6636)	0.4853 (0.6848)	0.5987 (0.7237)
TURNOVER	0.3165 (0.5239)	0.3389 (0.5330)	0.3490 (0.5373)	0.3156 (0.5333)	0.2554 (0.5479)
NB_INVOLVED	0.5983*** (0.1736)	0.6254*** (0.1773)	0.5867*** (0.1717)	0.5993*** (0.1739)	X
INVOLDED	X	X	X	X	1.5375*** (0.5569)
COMPETITORS	X	X	X	X	1.1348** (0.5654)
ORGANISME	X	X	X	X	X
NB_BENEF	0.3875** (0.1350)	0.3397** (0.1336)	0.3935** (0.1440)	0.3098** (0.1335)	0.2548** (0.1203)
NB_CHALL	-0.3223 (0.2129)	X	X	X	X
MANAGEMENT	X	X	-1.2745* (0.6843)	-1.2004 (0.7198)	X
ACTIONS	X	-1.9048** (0.8938)	X	-1.8055* (0.9912)	-2.1347** (0.9564)
NB_PRIORITY	0.1763 (0.2763)	0.1117 (0.2579)	-0.1153 (0.2530)	0.1346 (0.2534)	0.1734 (0.2634)
Number of observations	836	836	836	836	836
% concordance	87.4	87.6	87.4	88.4	87.7

Significance threshold: *** = 1% ; ** = 5% ; * = 10%.

Coefficient, the standard deviation in parentheses.

Chapter 8

Information Security Governance in Large Organizations: A Maturity Framework

ABSTRACT

There is a dearth of academic research literature on the practices and commitments of information security governance in organizations. Despite the existence of referential and standards of the security governance, the research literature remains limited regarding the practices of organizations and, on the other hand, the lack of a strategy and practical model to follow in adopting an effective information security governance. This chapter aims to discuss the information security governance and to address the weaknesses identified in the literature. Based on practices of information security management and governance, the authors propose ISGO, a practical maturity framework for the information security governance and management in organizations. The findings will help organizations to assess their capability maturity state and to address the procedural, technical, and human aspects of information security governance and management process.

DOI: 10.4018/978-1-5225-7826-0.ch008

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Many organizations today are facing a global governance revolution that could have a direct impact on their information management practices. Information security has become an integral part of daily life, and organizations must ensure that their information security systems are an integral part of daily life.

In a distributed and dynamic services environment, security must not be limited to providing technological solutions but to finding a strategy taking into account business, organizational and technological dimensions (Nassar, Badr, Barbar, & Biennier, 2009). In addition, security must be seen as an ongoing process that aims to optimise security investments and ensure the sustainability of the security measures implemented (Lomas, 2010). However, reference service domain models and architectures have underestimated the definition of security needs, the assets to be protected and the identification of risks to these assets (Huang, Lee, & Kao, 2006; Williams, 2007). For that, we propose to approach the problem of security by a practical approach of governance allowing to identify the various axes of my IT security and to propose the most adequate security measures to the context. However, IT security governance is a real challenge in an open collaborative services environment. In fact, improving security has emerged as one of the top IT priorities across all business lines. So, while companies (R. von Solms & van Niekerk, 2013; Bowen, Chew, & Hash, 2007).

Areas such as the aerospace industry and strategic resources can be ideal targets for cyber espionage by nation-states, others managing financial assets or large-scale credit card information are equally attractive to international criminal groups (Posthumus & von Solms, 2004; Humphreys, 2008). These malicious actors no longer content themselves with thwarting the means of technical protection. Instead, they survey and exploit a variety of weaknesses detected in the targeted environment (Galliers & Leidner, 2014). These shortcomings are not only technological but also result from failures in protection procedures or gaps in vulnerability management practices. The best technology in the world, if misused will not provide an adequate defence against such threats (R. von Solms & van Niekerk, 2013).

In today's rapidly changing and evolving environment, IT and security executives have to make difficult calculations and decisions about security with limited information (Dhillon, Syed, & Pedron, 2016). They need to make decisions that are based on analyzing opportunities, risks and security.

In such an environment, information security governance ISG issues are at the forefront of any discussions for security organization's information assets, which includes considerations for managing risks, data and costs. Organizations, worldwide, have adopted practical and applied approaches for mitigating risks and managing information security program (Y. Maleh, Sahid, Ezzati, & Belaissaoui, 2018; Yassine Maleh, 2018).

The problem is that the security governance framework is designed to guide organizations in their IS security governance strategy but does not define the practical framework for the engagement in this strategy. To address these concerns, some practice repositories (NIST, Cobit, ISACA, RiskIT) and international standards (ISO 27000 suite, ISO 15408) now include paragraphs on security governance. The first reports or articles in academic journals that evoke the governance of information security date back to the early 2000s. The proposed referential and best practices designed to guide organizations in their IT security governance strategy. However, does not define the practical framework to implement or to measure the organization engagement in term of IS security governance.

In this paper, we propose a practical framework to evaluate the organization in their maturity state and to improve their level of IS security governance according to their needs and resources. The article is structured as follows. Section 2 presents the theoretical framework. Section 3 describes the proposed capability maturity framework for information security governance ISGO. Section 4 discuss the results of the implementation of ISGO through a practical use case. Finally, section 6 presents the conclusion of this work.

THEORETICAL FRAMEWORK

Methodology

In the major modern organizations, it is no longer possible to ensure the security and governance of information assets on an ad hoc basis, or by deploying only technical solutions. Instead, these organizations need a holistic approach that applies effective risk management and good governance across the organization, and through which the fundamental values of visibility, accountability and responsibility are shared by all levels. Companies' efforts to improve security can motivate them to react and buy high-tech products that can make them more secure rather than more secure. The problem is that this

proliferation of advanced attacks does not allow you to be more responsive. Taking a more proactive approach to security involves the deployment of multiple layers of integrated protection that stifle network violations. The best approach is to make sure that your information security staff respond to new threats and your IT team member's process mature systems.

To responding to modern security challenges, organizations must continually apply effective risk management practices at all levels. Risks must be visible to senior management, who must play a fundamental role in accepting these risks or directing activities and allocating resources to reduce these risks to technically, commercially, legal, legislative and regulatory.

As described in the previous chapter of this book, our data are collected from large and medium companies on an international scale. There are several justifications for this choice.

ISG Frameworks

Governance first implemented by large firms, (Waddock & Graves, 1997) demonstrated that organizations with significant financial resources can invest more in strategic activities (Archibugi & Michie, 1995). Cohen (2006) stated that organizations must consider the security dimension in their strategy when they operating in a competitive environment, which is often the case for large enterprises. Moreover, SMEs has always shown an overall lack of security awareness (C. Mitchell, Marcella, & Baxter, 1999). They faced more serious problems than those encountered by large companies regarding security difficulties and a realistic assessment of the risks involved (Siponen & Willison, 2009; L. Goodhue & Straub, 1991; Peltier, 2013).

Moulton and Coles (2003) corporate governance and accountability are now at the top of government and investor agendas, not just in the US, but also throughout Europe and Asia. Chief Executives and Corporate Board's responsibilities for control are increasingly demanding. The Sarbanes Oxley law in the United States will require that all US-listed companies (including several of the world's largest companies with US lists) include reports on internal controls in their annual reports. Programs aimed to ensure compliance with the European legislation. They will have a significant impact on technology, and in particular on the governance of security. Also, financial institutions faced with the prospect of complying with the Basel II requirements.

Small and medium-sized enterprises have little security concern (Gupta & Hammond, 2005) and the vast majority of SMEs have no legal security

obligations to date. Securing SMEs is therefore always behind the big companies.

Hong, Chi, Chao, and Tang (2006) investigated the dominant factors for an organization to build an information security policy ISP, and whether an ISP may elevate an organization's security level in Taiwan. De Haes & Van Grembergen (2006) Interpreted some important existing practices and models in the IT governance field and derives open research questions and some research suggestions from it. They form the basis of the pilot case research in Belgian organizations. Lomas (2010) argued that by integrating ISO 27001 the international information security standard in co-occurrence with the ISO 15489 document management standard, holistic information governance strategies would provide a responsive response to changes in UK context. Bahl and Wali (2014) examine, as a case, the perceptions of the ISP's (Service Provider) in India regarding information security governance and its impact on the security service quality. Ula, Ismail, and Sidek (2011) propose an initial framework for governing the information security in the banking system. The framework classified into three levels: tactical level, strategic level, operational level and technical level. This proposed framework implemented in a banking environment. Mohamed and Singh (2012) propose a conceptual framework that examines information technology governance effectiveness, its determinants, and its impacts on private organizations.

Hung, Hwang and Liu (2013) proposed an ISG maturity model to search for relevant maturity characteristics of ISG. According to the information security assessment and maturity assessment tool, this study found that schools with a little maturity rate occupied 59.8%, 31.7% average and 8, 5%. With correlation analysis, this study concludes that 33 elements have a significant correlation with ISG maturity. With ANOVA, Post hoc scoping test, and ANOVA multiple comparative difference, this study finds that there are significant differences between the ISG maturity components. This study also found that the maturity of schools is basic. They can improve their information security governance maturity according to this model. Lunardi, Becker, Maçada and Dolci (2014) attempted to study and measure the improvement in the financial performance of firms that have adopted an IT management and governance strategies through pre- and post-adoption measures. They found that the organizational activities of improved IT governance practices boost their performance compared to the control group, particularly about profitability. They also concluded that the impact of adopting an IT management and

governance mechanisms on financial performance was more pronounced in the year following the adoption than in the year in which they took.

Adéle da Veiga and Martins (2015) discussed through a case study of an international financial institution in which ISCA conducted at four intervals over a period of eight years in twelve countries. Multivariate and comparative analyses performed to determine whether the culture of information security has improved from one evaluation to another depending on the development actions implemented. One of the primary measures performed was training and awareness-raising on the critical dimensions identified by ISCA. The culture of information security has improved from one evaluation to another, with the most positive results in the fourth assessment.

Dhillon, Syed and Pedron (2016) used Hall's theory of cultural message flows (1959) to evaluate disturbances in the security culture following a merger. They conducted an exhaustive case study of a company in the telecom sector. The data were collected during the merger, allowing us to evaluate the changing structures in real time. The results of this analysis help researchers and practitioners to theorize on the formulation of security culture during a merger. On the practical side, decision-makers will find this analysis useful for engaging in strategic security planning. Eroğlu and Çakmak (2016) measured information systems regarding information security and risk. On the other hand, it also aims to describe the potential effects of evaluation techniques and tools for state organizations to manage their critical assets. The information systems of one of the major healthcare organizations in Turkey have evaluated through an international assessment tool adapted to Turkish specificities and conditions in certain parts of the legal regulations. The results obtained through an evaluation tool provide the current level of maturity of the organization and point out areas that should improve the security of information systems and essential components such as risks, processes, people, IT dependence and technology.

In recent works, Dhillon, Syed, and Sá-Soares (2017) identified information security concerns in information technology (IT) outsourcing and analyzed the (in) congruence between customers and suppliers with respect to these concerns. Moody, G. D., Siponen, and Pahlila (2018) reviewed 11 theories that have been used in most previous models of information security behaviour to propose a unified model, called the Unified Information Security Policy Compliance Model (UMISPC).

ISG BEST PRACTICES

An ISG frameworks can be successfully implemented by adopting best practices (Williams, 2001). S. H. Von Solms (2005) indicated that companies realize that instead of trying to establish an information security governance environment on an ad hoc basis, it is preferable to follow an internationally recognized framework. There are several resources that can be used as a guide for information security governance, for example:

- Control Objectives for Information Technology and Related Technologies (COBIT) that helps mitigate risk, assess maturity of strategic alignment and value of IT delivery (Mataracioglu, T., & Ozkan, 2011; Raup-Kounovsky, Canestraro, Pardo, & Hrdinová, 2010; Saetang & Haider, 2011; Simonsson, Lagerström, & Johnson, 2008)
- National Institute of Standards and Technology (NIST) (IT Governance) 2008 ; (Dlamini, Eloff, & Eloff, 2009).
- International Organization for Standardization (ISO)/International Electro technical Commission (IEC) 27000 family of safety standards (ITG, 2008) such as ISO17799 (Spafford, 2003) and ISO27001 (Mataracioglu, T., & Ozkan, 2011)
- Certified Information Systems Security Professional (CISSP) (Harris, 2007)

B. Von Solms (2005) discussed the advantages and disadvantages of using COBIT and ISO17799 and stated that both are good choices for information security governance and are complementary and therefore, when used together, can bring benefits to the organization. COBIT allows information security to be integrated into a broader IT framework, which means that if the company decides to implement the rest of the framework, it is available. COBIT, however, focuses on what needs to be done, but does not provide detailed guidelines on how to do it. ISO17799, on the other hand, provides more detailed guidance on how things should be done, but only addresses information security and is not integrated into a broader IT governance framework. It is the only framework that allows an organization to obtain third-party audit certification (Saint-Germain, 2005).

The IT Governance Institute (ITG, 2008) recommended that a framework be established and maintained by management to guide the development and maintenance of an information security program to achieve effective information security governance. (Spafford, 2003) described a number of compelling reasons why organizations should instead adopt existing standards, such as a well-defined structure, that they have been developed and evaluated over many years by many individuals and organizations. They provide a platform for knowledge sharing among organizations, and that they facilitate the certification of organizations against a basic standard from which improvements can be recommended.

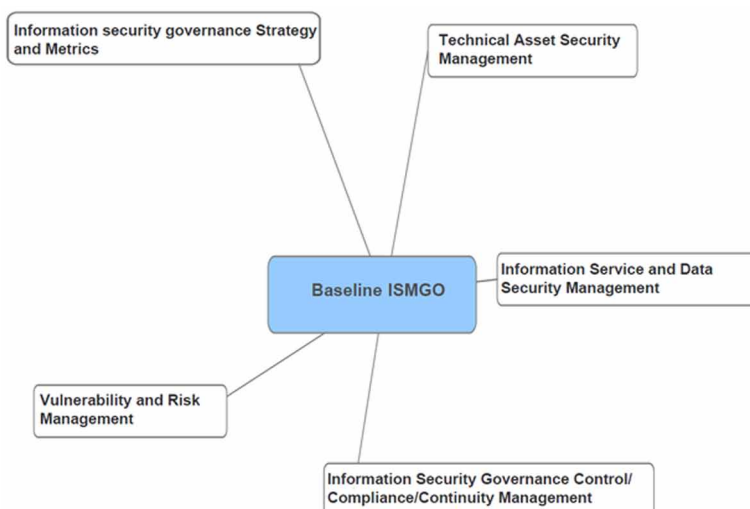
In this next section, we present an ISGO capacity maturity framework focused on practitioners that integrate the technical, process and human dimensions. The framework is based on the fact that the pace and manner in which an organization can respond proactively to new and emerging security threats depends on the maturity of its ISGO capacity. The fundamental pillars of the ISGO must be fluid and responsive to the changing landscape of information security; by developing their capabilities to detect, assess and respond to new and emerging security threats, organizations can position themselves more proactively to efficiently and continuously secure information resources.

Framework Overview

We propose a global maturity framework to achieve an effective information security governance and governance approach, as shown in Figure 1. The path to security maturity requires a diversified range of layered endpoint protection, management and capabilities, all integrated and fully automated. The only practical and survivable defensive strategy are to move to a more mature security model that incorporate multiple layers of protective technology.

The ISGO framework focuses on determining the capacity of an organization to direct oversee and monitor the actions and processes necessary to protect documented and digitised information and information systems and to ensure protection against access, unauthorized use, disclosure, disruption, alteration or destruction, and to guaranty confidentiality, integrity, availability, accessibility and usability of the data (Kenneally, Jim Curley, 2012). The framework extends the triad confidentiality, integrity and availability of commonly cited with accessibility and usability concepts. Concerning accessibility, a failure to support and understand how security can change work practices

Figure 1. The proposed maturity framework for information security governance in organizations ISGO



can impede how data and information are accessed, shared, and acted on in an increasingly dynamic, competitive environment. Similarly, usability is a one of a main key factor to engaging stakeholders in the business processes, independently of the availability of technology to support work practices, if the technology is difficult to interact and engage with, users might adopt other locally developed, less secure methods of access. The proposed Information Capability Maturity Framework is a comprehensive suite of proven management practices, assessment approaches and improvement strategies covering 5 governance capabilities, 21 objectives and 80 controls.

Framework Core

The ISGO framework classifies the information security activities across the following five high-level function categories:

- Information security strategy and governance provide the oversight structures for supporting ISGO; it implements information security strategy, policies, and controls; assigns. Define roles and responsibilities for ISGO activities; provides communication and training; reports on ISGO activities' effectiveness; and manages supplier security

Information Security Governance in Large Organizations

requirements; plans and tests the security of business continuity measures.

- Technical asset security management establishes a security architecture and implements measures to control IT component and physical infrastructure security.
- Information services, system and data management, provides security budgets, tools, and resources, and measures the resource efficiency of security investments. Defines data security classifications and provides guidance on managing access rights and data throughout its lifecycle.
- Vulnerability and risk management to control profiles security threats and assesses priorities, handles, and monitors security-related risks.
- Information security compliance, control and verification.

As Table 1 shows, these high-level function categories are decomposed into 21 security practice objectives (SPOs).

Table 1. ISGO functions and objectives

Governance Functions	Security Practice Objective	Description
Information security governance Strategy and Metrics	Information Security Strategy and policies	Develop, communicate, and support the organization's information security objectives. Establish and maintain security policies and controls, taking into account relevant security standards, regulatory and legislative security requirements, and the organization's security goals.
	Strategic alignment of security	From risk analysis to the actual deployment of global policy, security must be aligned with the business priorities of the company while respecting regulatory and legal constraints
	Communication and Training	Disseminate security approaches, policies, and other relevant information to develop security awareness and skills.
	People Roles and responsibilities	Document and define the responsibilities and roles for the security of employees, contractors and users, by the organization's information security strategy.
	Security performance assessment	Report on the efficiency of information security policies and activities, and the level of compliance with them.
	Assessment of security budget and investments	Provide Security related investment and budget criteria.
Technical Asset Security Management	Security architecture	Build security measures into the design of IT solutions—for example, by defining coding protocols, depth of defense, the configuration of security features, and so on.
	IT component Security	Implement measures to protect all IT components, both physical and virtual, such as client computing devices, servers, networks, storage devices, printers, and smartphones.
	Physical Infrastructure Security	Establish and maintain measures to safeguard the IT physical infrastructure from harm. Threats to be addressed include extremes of temperature, malicious intent, and utility supply disruptions.

continued on following page

Table 1. Continued

Governance Functions	Security Practice Objective	Description
Information Service/ System/Data Security Management	Incident Management	Manage security-related incidents and near-incidents. Develop and train incident response teams to identify and limit exposure, manage communications, and coordinate with regulatory bodies as appropriate.
	Resource Effectiveness	Measure “value for money” from security investments; capture feedback from stakeholders on the effectiveness of security resource management.
	Data identification and Classifications	Define information security classes, and provide guidance on protection and access control appropriate to each level.
	Access Management	Manage user access rights to information throughout its lifecycle, including granting, denying, and revoking access privileges.
	System Acquisition, Development, and Maintenance Security Policy	Ensure the management of security throughout the life cycle of Information Systems. Reduce risks related to exploiting technical vulnerabilities and applications.
Vulnerability and Risk Management	Security Threat profiling	Gather intelligence on IT security threats and vulnerabilities to better understand the IT security threat landscape within which the organization operates, including the actors, scenarios, and campaigns that might pose a threat.
	Security Risk Assessment	Identify exposures to security-related risks, and quantify their likelihood and potential impact.
	Security Risk Prioritization	Prioritize information security risks and risk-handling strategies based on residual risks and the organization’s risk appetite.
	Security Monitoring	Manage the ongoing efficacy of information security risk-handling strategies and control options.
Information Security Governance Control/ Compliance/Continuity Management	Compliance Control	Identify applicable law, statutory and contractual obligations that might impact the organization. Establish security and compliance baseline and understand per-system risks.
	Security Testing and Auditing	Adopt solution for information security audit. Establish project audit practice. Derive test cases from known security requirements
	Business continuity planning	continuity management Business continuity planning Provide stakeholders throughout the organization with security advice to assist in the analysis of incidents and to ensure that data is secure before, during, and after the execution of the business continuity plan.

Framework Maturity Profile

The bottom line on information security is that the threat environment of today is simply too dynamic. The only practical and survivable defense strategy are to move to a more mature security model that integrate multiple layers of protection technology.

We propose a mature and systematic approach to information security governance. Adopting a security maturity strategy requires a full range of protection, management and defensive features that must be integrated and capable of fully automated operation.

Concerning each security practice objectives SPO outlined in Table 2, the framework defines a five-level of maturity that serves as the basis for understanding an organization's ISGO capability and provides a foundation for capability improvement planning.

Level 0 - None: No process or documentation in place.

Level 1 - Initial: Maturity is characterized by the ad hoc definition of an information security strategy, policies, and standards. Physical environment and IT component security are only locally addressed. There is no explicit consideration of budget requirements for information security activities, and no systematic management of security risks. Access rights and the security of data throughout its lifecycle are managed at best using informal procedures. Similarly, security incidents are managed on an ad hoc basis.

Level 2 – Basic: Maturity reflects the linking of a basic information security strategy to business and IT strategies and risk appetite in response to individual needs. It also involves the development and review of information security policies and standards, typically after major incidents. IT component and physical environment security guidelines are emerging. There is some consideration of security budget requirements within IT, and requirements for high-level security features are specified for major software and hardware purchases. A basic risk and vulnerability management process are established within IT according to the perceived risk. The access rights control and management depend on the solutions provided by the provider. Processes for managing the security of data throughout its life cycle are emerging. Major security incidents are tracked and recorded within IT.

Level 3 - Defined: Maturity reflects a detailed information security strategy that's regularly aligned to business and IT strategies and risk appetite across IT and some other business units.

Information security policies and standards are developed and revised based on a defined process and regular feedback. IT and some other business units have agreed-on IT component and physical environment security measures. IT budget processes acknowledge and provide for the most important information security budget requests in IT and some other business units. The security risk-management process is proactive and jointly shared with corporate collaboration. Access rights are granted based on a formal and audited authorization process. Detailed methods for managing data security

throughout its life cycle are implemented. Security incidents are handled based on the urgency to restore services, as agreed on by IT and some other business units.

Level 4 – Managed: Maturity is characterized by regular, enterprise-wide improvement in the alignment of the information security strategy, policies, and standards with business and IT strategies and compliance requirements. IT component security measures on IT systems are implemented and tested enterprise-wide for threat detection and mitigation. Physical environment security is integrated with access controls and surveillance systems across the enterprise. Detailed security budget requirements are incorporated into enterprise-wide business planning and budgeting activities. A standardized security risk-management process is aligned with a firm risk-management process. Access rights are implemented and audited across the company. Data is adequately preserved throughout its life cycle, and data availability is effectively requirements. Recurring incidents are systematically addressed enterprise-wide through problem-management processes that are based on root cause analysis.

Level 5 – Optimized: Maturity reflects an information security strategy that is regularly aligned to business and IT strategies and risk appetite across the business ecosystem. Information security policies and standards are periodically reviewed and revised based on input from the business ecosystem. The management of IT component security is optimized across the security framework layers. Physical access and environmental controls are regularly improved. Security budget requirements are adjusted to provide adequate funding for current and future security purposes. The security risk-management process is agile and adaptable, and tools can be used to address the business ecosystem's requirements. The access rights control and management are dynamic and can effectively deal with the organizational restructuring of acquisitions and divestitures. Processes for managing data security throughout its life cycle are continuously improved. Automated incident prediction systems are in place, and security incidents are effectively managed.

USE CASE: APPLYING THE PROPOSED FRAMEWORK FOR INFORMATION SECURITY GOVERNANCE (ISGO)

The pre-established questionnaire took into account the realities of the organization. At the end of this survey, and following a metric, we were able to evaluate the deviations from the norm and to assess the level of maturity regarding security concerning the different axes of our framework. The audit questionnaire consists of 100 questions divided into different objectives and control of the information security governance inspired by best practice guides ISO 27001 (Johnson, 2014) and OWASP (Deleersnyder et al., 2009). Each item is assigned a weighting coefficient on the effectiveness of the rule of the reference system to which the question relates regarding risk reduction. After the validation of the Questionnaire, the chosen answers were introduced in the software maturity framework that was used to allow the automation of the processing and to determine the maturity score. The treatment consists of calculating a weighted average of the scores obtained according to the chosen responses and the efficiency coefficient. The result is a numerical result (0 to 5 or expressed as a percentage) representing the level of security (maturity) of the audited IS.

Data Collection

The questionnaire was carried out in several stages. A first version has been developed to take into account the different theoretical assumptions. This first version has been tested with IT service managers and consultants. This pre-test allowed rephrasing some questions to improve the comprehension of the questionnaire and to improve the quality of the given answers. In the end, the questionnaire consists of 100 questions divided into different security objectives and controls.

Data Analysis

The pre-established questionnaire took into account the realities of the organization. At the end of this survey, and following a metric, the authors were able to evaluate the deviations from the norm and to assess the level of ISG maturity regarding concerning the different axes of the framework. The audit questionnaire consists of 110 questions divided into different ITSG objectives and controls inspired by best practice guides ISO 27000 (Johnson,

Table 2. Organization background

	Year	Frequency
Size of the Company (# of Employees)	2017	More than 1,200
Position	Senior Executives	460
	Executives	95
	Lower Management	420
	Qualified non-supervisory	146
	Non-supervisory	79
Evolution of Turnover and Revenue of the Company for the last 5 years in \$	2012	More than 1,5 million
	2013	Fewer than 3 million
	2014	More than 1,7 million
	2015	More than 1,5 million
	2016	Fewer than 2 million
	2017	More than 2 million

Table 3. Participants' demographics

Participants	Frequency	Percent
Male	68	68,42%
Female	36	31,58%
Top manager personnel	17	14,91%
Senior Manager	23	20,18%
IT Manager	7	6,14%
Consultant/Engineer/Analyst	13	11,40%
IT Technical Staff	19	16,67%
Helpdesk Technician	7	6,14%
Quality Assurance / Quality Control	15	13,16%
Other entities staff	13	14,91%

2014) and COBIT (Deleersnyder et al., 2009). Each item is assigned a weighting coefficient on the effectiveness of the rule of the reference system to which the question relates regarding risk reduction. After the validation of the Questionnaire, the chosen answers were introduced in the software maturity framework that was used to allow the automation of the processing and to determine the ISG maturity score. The treatment consists of calculating a weighted average of the scores obtained according to the chosen responses and

the efficiency coefficient. The result is a numerical result (0 to 5 or expressed as a percentage) representing the level of maturity of the audited ISG.

Conducting Assessments

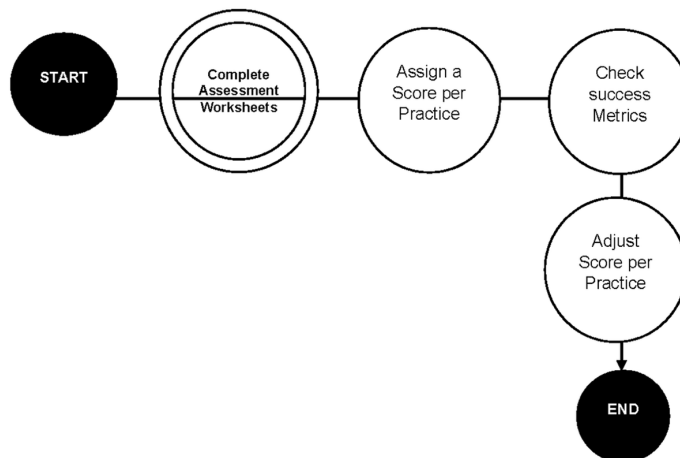
By measuring an organization based on defined security practices, a comprehensive picture of integrated security assurance activities is created. This type of evaluation is useful for understanding the extent of the security activities currently in place in an organization. Also, it allows the organization to use the maturity framework to create a future roadmap for continuous improvement.

An important first step of the assessment is to define the assessment scope. An assessment can be carried out for a complete organization or selected business units. This scope should be agreed with the key stakeholders involved.

Scoring an organization using the evaluation spreadsheets is simple. After answering questions, assess the answer column to determine the score. Insurance programs may not always consist of activities that fall carefully over a limit between maturity levels.

An organization will receive credit for the different levels of work it has performed in practice. The score is fractional to two decimal places for each practice and one decimal for a response. Questions were also changed from Yes / No to five options related to maturity levels. Anyone who completed the assessment discussed whether to report a yes or no answer when it is honestly something in between.

Figure 2. Conducting assessment model



The toolbox worksheet contains contextual answers for each question in the assessment. The formulas in the toolbox will average the answers to calculate the score for each practice, a loop average for each business function and an overall rating. The toolkit also features dashboard graphics that help to represent the current score and can help show program improvements when the answers to the questions change. An example of an evaluation calculation can be found in Appendix 2.

The framework's assessment tool provides a granular and focused view of an organization's current maturity state for each SPO, desired or target maturity state for each SPO, and importance attributed to each SPO. These maturity and significance scores are primarily determined by an online survey undertaken by the organization's key IT and business stakeholders (See Appendix 1). The survey typically takes each assessment participant 30–45 minutes to complete, and the data collected can be augmented by qualitative interview insights that focus on issues such as key information-security related business priorities, successes achieved, and initiatives taken or planned. The assessment provides valuable insight into the similarities and differences in how key stakeholders view both the importance and maturity of individual SPOs, as well as the overall vision for success. Figure 4 shows the results of an organization's ISGO capability maturity assessment, outlining its current and target SPO maturity across all 21 SPOs. For each SPO, the maturity results are automatically generated by the proposed assessment tool, based on averaging the survey participants score across all questions about that SPO. Based on this average score achieved, the organization highlighted in Figure 4 reflects a level 1.4 (initial) current maturity status for ISGO overall, but it is less mature in some SPOs, such as security budgeting, resource effectiveness, security threat profiling, and security risk handling. Based on the average across all SPOs, its desired target ISGO maturity state is maturity level 2.4 (Basic) for the first 6 month after the first organization assessment.

Figure 3. Assessment score

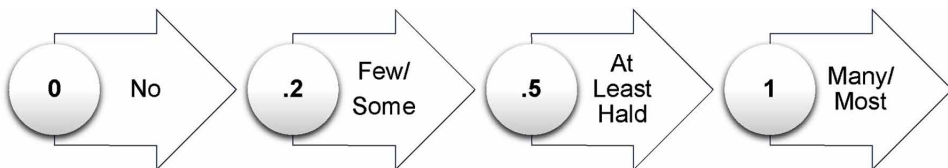
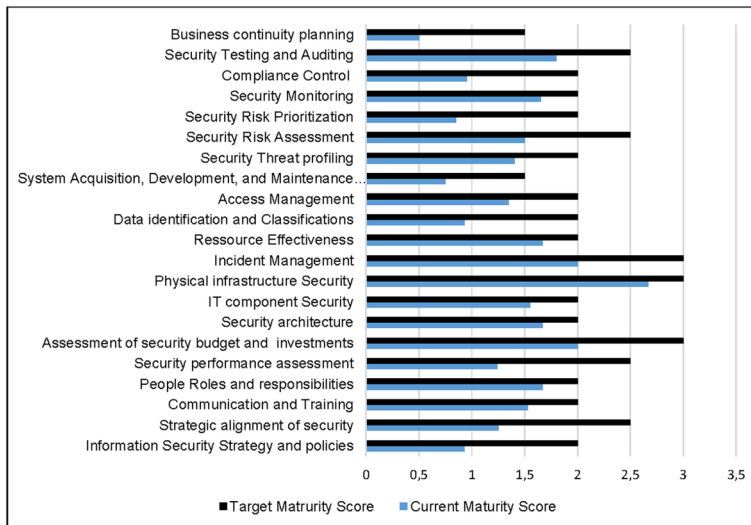


Figure 4. The proposed information security governance assessment results



The output from the framework’s assessment supports understanding the actions necessary to drive improvement and enable the organization to transition from its current to target maturity state systematically. This is achieved by implementing a series of industry-validated practices that allow organizations to improve incrementally and monitoring and tracking progress over time using a number of industry-validated metrics. Table 4 includes sample practices and metrics for the 5 SPOs highlighted for prioritized improvement. For each of these SPOs, the figure outlines the currently reported maturity and the practices required to transition to the next maturity state. Note that additional practices are available to support transitioning to the desired maturity state.

To reach the target maturity levels score, the organization adopted an action plan Plainfield over 3 phases in 2 years from 2016 to 2018 as shown in Table 5.

To reach the desired level of maturity. The organization implemented some programs during each phase of the rollout. The following initiatives were adopted for the first phase (Months 0-6):

- Construct a white paper of technical guidance for application security on the technologies used within the organization.
- Create a risk process and conduct high-level business risk assessments for application platforms and review the business risk.

- Prepare initial guidelines and technical standards for developers.
- Conduct short implementation reviews on application platforms that pose a significant risk to the organization.
- Develop test cases and use cases for projects and evaluate arguments against applications.
- Created a role in application security initiatives.
- Generated a strategic roadmap for the next phase of the security program.

Table 4. Example practices and metrics to drive improvement in specific security practice blocks (CSPBs)

Governance Functions	Control Objective	Current Maturity Score	Target Maturity Score	Target Objectives to Increase Maturity Score	Metrics
Information security governance Strategy and Metrics	Information Security Strategy and policies	0,93	2	Develop basic information security strategies that consider IT and business strategies and risk appetite. Build and maintain technical guidelines	Existence and availability of security strategies that include business and IT strategies and risk appetite Number and percent of stakeholders aware of and using information security strategies
	Strategic alignment of security	1,25	2,5	Align the governance strategy of security with the organization's overall IT governance strategy.	Control objectives tied to specific strategic and business objectives.
	Communication and Training	1	2	Conduct technical security awareness training	Employee satisfaction surveys. % staff trained within the past year. % Analyst/management staff trained within the previous year.
	People Roles and responsibilities	1,67	2,8	A clear assignment of responsibilities with information security	System accounts-to-employees ratio. Security awareness level. Psychometrics.
	Security performance assessment	1,24	2,5	Develop a measurement dashboard and regular monitoring of the performance security if the body regarding availability, integrity, confidentiality and non-repudiation	A number of controls meeting defined control criteria/objectives. % of controls that are ossified or redundant.
	Assessment of security budget and investments	2	3	Estimate overall business risk profile	IRR (Internal Rate of Return). The annual cost of information security controls. ROI (Return On Investment). ROSI (Return on Security Investment)

continued on following page

Information Security Governance in Large Organizations

Table 4. Continued

Governance Functions	Control Objective	Current Maturity Score	Target Maturity Score	Target Objectives to Increase Maturity Score	Metrics
Technical Asset Security Management Information Service/System/ Data Security Management	Security architecture	1,67	2,4	Identify and promote security services and design patterns from architecture	% of project report, model, platform, and pattern usage feedback. % of project teams informed about appropriate security standards.
	IT component Security	1,55	2,4	Identify, inventory and classify all assets needed for information management. For each of them, a manager must be determined. It is responsible for enforcing the security policy for its assets.	Discrepancies between logical access location and physical location. A number of unacceptable physical risks on premises. % of IT devices not securely configured
	Physical Infrastructure Security	2,67	3,5	Ensure the protection and availability of sensitive equipment. Ensure that only authorized persons have access to the buildings, technical premises and archives of the organization and that access is traced	Number IT assets without an owner. % of information assets not [correctly] classified
Information Service/System/ Data Security Management	Incident Management	2	3	Prioritize and manage security incidents based on the urgency to restore services. Identify indicators and establish security incidents Dashboards	A number of information security events and incidents, major and minor. IT security incidents cumulative cost to date. Non-financial impacts and effect of IT incidents.
	Resource Effectiveness	1,5	2	Identify and classify data based on criticality, business risk, etc	% of data by the degree of criticality.
	Data identification and Classifications	0,93	2	Establish a process to withdraw employee access rights if abused. Discourage sharing of credentials. Provide employees with access to a password-management package.	A Number of access rights audit exceptions. A Number of grant/revoke of access rights by the department.
	Access Management	1,35	2	Conduct basic intelligence gathering and create basic threat profiles.	% of inactive user accounts disabled by policy.
	System Acquisition, Development, and Maintenance Security Policy	0,75	1,5	Access control to applications/programs source code. Restrictions on modifications to software Packages.	% of controls tested practically. % of technical security checks.

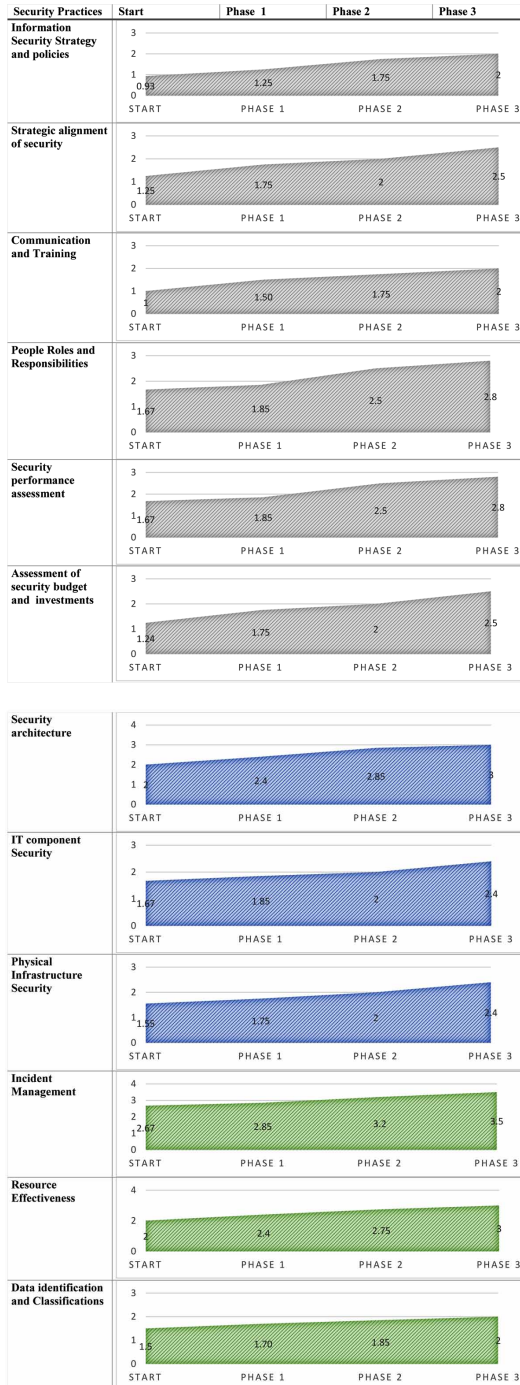
continued on following page

Table 4. Continued

Governance Functions	Control Objective	Current Maturity Score	Target Maturity Score	Target Objectives to Increase Maturity Score	Metrics
Vulnerability and Risk Management	Security Threat profiling	1,4	2	Create and conduct high-level risk assessments for application platforms and review business risk.	A number of unpatched vulnerabilities. IT security risk scores.
	Security Risk Assessment	1,5	2,5	Develop an application prioritization approach that identifies "static" risks and "relative" risk of each application	A number of small, medium and high/ risks currently untreated/unresolved. Number of attacks
	Security Risk Prioritization	0,85	2	Implement Security Monitoring and Analytics tool to quickly detect, analyze and correct the widest range of threats to the organization's IT resources.	Application Availability Rates. IT Application Total Downtime. Average Response Time of IT components.
Information Security Governance Control/ Compliance/ Continuity Management	Security Monitoring	1,65	2,2	Avoid the violation of intellectual property, legal, regulatory, contractual and organizational security requirements.	Historical consequences of noncompliance. Status of compliance with internally mandated (corporate) information security requirements. Number or rate of security policy noncompliance infractions detected
	Compliance Control	0,95	2	Derive test cases from known security requirements Conduct audit and penetration testing on software releases	Number and severity of findings in audit reports, reviews, assessments etc.
	Security Testing and Auditing	1,8	2,5	Following a minor incident (failure of equipment), ensuring the IT back depending on business needs. Following a major incident impacting the whole of a machine room, ensure a continuity of computer activity of the sensitive goods in the shortest time and according to the needs of the trades	Disaster recovery test results. Business continuity plan for maintenance status

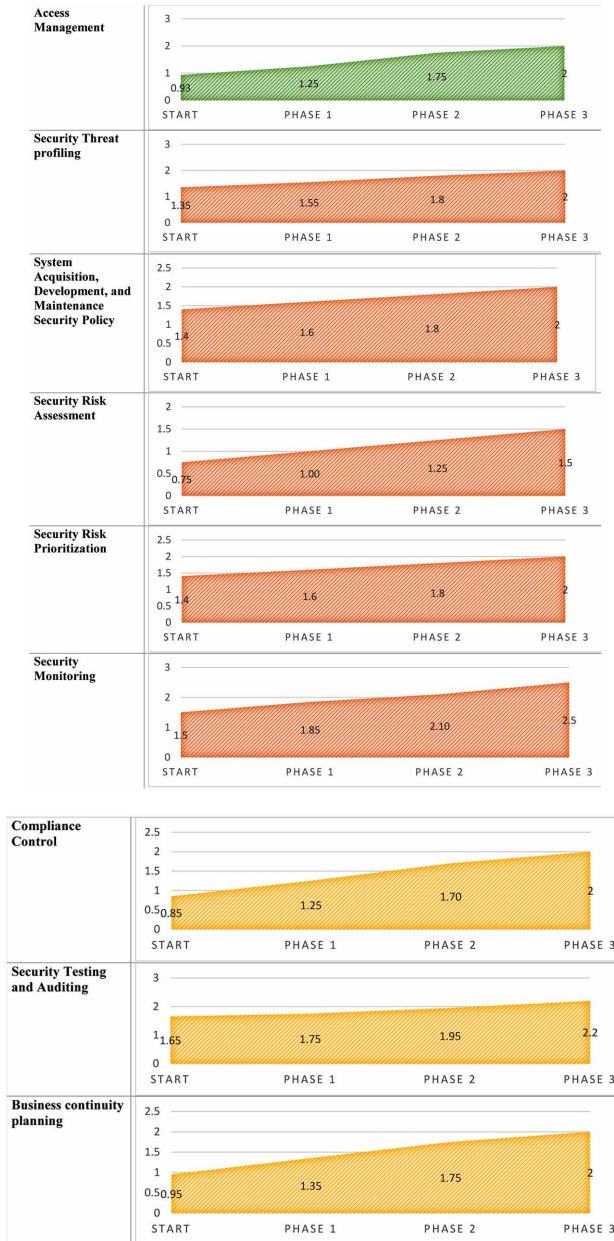
Information Security Governance in Large Organizations

Table 5. Governance maturity assessment roadmap



continued on following page

Table 5. Continued



Due to limited expertise in the intern, the company partnered with a third-party safety consulting group to assist in the creation of the training program and helped to elaborate a threat modeling and a strategic security roadmap.

The organization was aware that they had applications with vulnerabilities and no real strategy to identify existing vulnerabilities or resolve risks within a reasonable timeframe. A methodology based on risk assessment was adopted, and the organization undertook a review of existing application platforms.

This phase also included the implementation of a number of concepts for the IT team to improve their security tools. IT teams already had a number of tools in place for quality assessments. An additional survey of code review and security testing tools was conducted. During this phase of the project, the organization will implement the following security maturity practices & activities as shown in Table 6.

LIMITATIONS AND FUTURE WORKS

There are a number of limitations to this study. The study on the practices and commitment of organizations regarding security governance has been carried out over a range of 1000 medium and large size organizations (as described in the previous chapter). While some SMEs, especially those for

Table 6. Target objectives of phase 1 (Months 0-6) to achieve the target maturity level

Governance Functions	Target goals (Months 0-6)
Information security governance Strategy and Metrics	<ul style="list-style-type: none"> - Establish and maintain of assurance and protection program roadmap. - Classify applications and information based on business-risk - Ensure data owners and appropriate security levels are defined.
Technical Asset Security Management	<ul style="list-style-type: none"> - Derive security requirements from business functionality. - Ensure asset management system and process for hardware and software.
Information Service and Data Security Management	<ul style="list-style-type: none"> - Identify, inventory and classify all assets needed for data management. - Define and maintain appropriate security levels.
Vulnerability and Risk Management	<ul style="list-style-type: none"> - Ensure that Standards are implemented on all machines, has current definitions and appropriate settings. - Ensure users are periodically informed of unit virus prevention policies.
Information Security Governance Control/Compliance/Continuity Management	<ul style="list-style-type: none"> - Ensure documented control processes are used to ensure data integrity and accurate reporting. - Ensure periodic system self-assessments/risk assessments, and audits are performed. - Ensure the identification and monitoring of external and internal compliance factors.

which information is the heart may be practicing governance of information security. The survey of such a sample could be an interesting extension of the research.

After that, there may be a question of generalization for the organizations for each sector of activity and by specific region. In particular, the relative cost of technology to the workforce varies and thus influences the patterns of security spending. However, there is a high probability that the attitudes and beliefs of security managers regarding the security strategy will be similar in all countries.

Organizations that have a vast knowledge of the sensitivity of their experience can approach the security strategy differently, but no indication has been found in the literature review.

In the second phase of this research project, a model for measuring the maturity of the governance of the information system was proposed and implemented in a medium-sized organization. The results are satisfactory and prove that the model will be able to provide great support to organizations in different sizes and various sectors of activity in their governance and management of information security. Nevertheless, it is suggested that the scientific community and organizations adopt this framework and test it in different case studies.

CONCLUSION

This paper proposes a framework for measuring the maturity of information security was proposed with the aim of providing a practical tool for measuring and improving governance of information security in the organization. ISGO has been implemented in a medium organization to drive and improve ISGO maturity. The results are satisfactory and prove that the model will be able to provide great support to organizations in different sizes and various sectors of activity in their governance and management of information security. Nevertheless, it is suggested that the scientific community and organizations adopt this framework and test it in different case studies.

This research has shown how organizations implement information security governance. A grounded case study strategy answered the research question and developed practice using the procedures and techniques of grounded practice methodology discussed in the previous chapter of this book.

While existing research has focused on the implementation of information security governance and it is recognized that it is not possible to have a completely secure environment, research has found that the close relationship between risk management, information security governance, and compliance is critical to achieving objectives.

The last chapter of this section investigates what controls of ISO 27002 are commonly used and how they are selected to the implementation of an effective information security through a case study in a large organization of MENA region.

REFERENCES

- Archibugi, D., & Michie, J. (1995). Technology and Innovation: An Introduction. *Cambridge Journal of Economics* (Vol. 19). doi:10.1093/oxfordjournals.cje.a035298
- Bowen, P., Chew, E., & Hash, J. (2007). *Information Security Guide For Government Executives Information Security Guide For Government Executive*. National Institute of Standards and Technology NIST. doi:10.6028/NIST.IR.7359
- Cohen, F. (2006). *IT Security Governance Guidebook With Security Program Metrics*. Pennsauken, NJ: Auerbach Publishers Inc. doi:10.1201/b15999
- De Haes, S., & Van Grembergen, W. (2006). Information technology governance best practices in Belgian organisations. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 8. 10.1109/HICSS.2006.222
- Deleersnyder, S., De Win, B., Glas, B., Arciniegas, F., Bartoldus, M., & Carter, J. (2009). *Software Assurance Maturity Model*. Academic Press.
- Dhillon, G., Syed, R., & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management*, 54(4), 452–464. doi:10.1016/j.im.2016.10.002
- Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, 56, 63–69. doi:10.1016/j.cose.2015.10.001

- Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, 28(3), 189–198. doi:10.1016/j.cose.2008.11.007
- Galliers, R. D., & Leidner, D. E. (2014). Strategic information management: challenges and strategies in managing information systems. *Information Strategy*, 625. Retrieved from <http://www.worldcat.org/isbn/0750656190>
- Goodhue, D., & Straub, D. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management* (Vol. 20). doi:10.1016/0378-7206(91)90024-V
- Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security*, 13(4), 297–310. doi:10.1108/09685220510614425
- Harris, S. (2007). *CISSP certification all-in-one. Exam Guide* (4th ed.). New York: McGraw-Hill Publishing.
- Hong, K., Chi, Y., Chao, L. R., & Tang, J. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, 14(2), 104–115. doi:10.1108/09685220610655861
- Huang, S., Lee, C.-L., & Kao, A.-C. (2006). Balancing performance measures for information security management: A balanced scorecard framework. *Industrial Management and Data Systems* (Vol. 106). doi:10.1108/02635570610649880
- Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, 13(4), 247–255. doi:10.1016/j.istr.2008.10.010
- ITG. (2008). *Information Security Governance: Guidance for Information Security Managers*. Retrieved July 10, 2012, from http://www.globalteksecurity.com/SEGURIDAD_EN_LA_NUBE%20%20VIRTUALIZACION/Information%20Security%20Governanc
- Johnson, B. G. (2014). *Measuring ISO 27001 ISMS processes*. Academic Press.

- Lomas, E. (2010). Information governance: Information security and access within a UK context. *Records Management Journal*, 20(2), 182–198. doi:10.1108/09565691011064322
- Maleh, Y. (2018). Security and Privacy Management, Techniques, and Protocols. IGI Global. doi:10.4018/978-1-5225-5583-4
- Maleh, Y., Sahid, A., Ezzati, A., & Belaisaoui, M. (2018). A capability maturity framework for IT security governance in organizations. *Advances in Intelligent Systems and Computing*, 735, 221–233. doi:10.1007/978-3-319-76354-5_20
- Mataracioglu, T., & Ozkan, S. (2011). *Governing information security in conjunction with COBIT and ISO 27001*. arXiv Preprint arXiv:1108.2150.
- Mitchell, R., Marcella, R., & Baxter, G. (1999). Corporate information security management. *New Library World* (Vol. 100). doi:10.1108/03074809910285888
- Mohamed, N., & Singh, J. K. (2012). A conceptual framework for information technology governance effectiveness in private organizations. *Information Management & Computer Security*, 20(2), 88–106. doi:10.1108/09685221211235616
- Moody, G. D., Siponen, M., & Pahlila, S. (2018). Toward a unified model of information security policy compliance. *Management Information Systems Quarterly*, 42(1), 285–311. doi:10.25300/MISQ/2018/13853
- Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, 22(7), 580–584. doi:10.1016/S0167-4048(03)00705-3
- Nassar, P. B., Badr, Y., Barbar, K., & Biennier, F. (2009). Risk management and security in service-based architectures. In *2009 International Conference on Advances in Computational Tools for Engineering Applications* (pp. 214–218). Academic Press. 10.1109/ACTEA.2009.5227927
- Peltier, T. R. (2013). *Information Security Fundamentals* (2nd ed.). Taylor & Francis. doi:10.1201/b15573
- Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 23(8), 638–646. doi:10.1016/j.cose.2004.10.006

- Raup-Kounovsky, A., Canestraro, D. S., Pardo, T. A., & Hrdinová, J. (2010). IT Governance to Fit Your Context: Two U.S. Case Studies. In *Proceedings of the 4th International Conference on Theory and Practice of Electronic Governance* (pp. 211–215). New York: ACM. 10.1145/1930321.1930365
- Saetang, S., & Haider, A. (2011). Conceptual Aspects of IT Governance in Enterprise Environment. In *Proceedings of the 49th SIGMIS Annual Conference on Computer Personnel Research* (pp. 79–82). New York: ACM. 10.1145/1982143.1982164
- Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *The Information Management Journal*, 39(4), 60–66.
- Simonsson, M., Lagerström, R., & Johnson, P. (2008). A Bayesian Network for IT Governance Performance Prediction. In *Proceedings of the 10th International Conference on Electronic Commerce* (p. 1:1--1:8). New York: ACM. 10.1145/1409540.1409542
- Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), 267–270. doi:10.1016/j.im.2008.12.007
- Spafford, G. (2003). *The benefits of standard IT governance frameworks*. Retrieved April 4, 2012, from http://www.itmanagementonline.com/Resources/Articles/The_Benefits_of_Standard_IT_Governance_Frameworks.pdf
- Ula, M., Ismail, Z., & Sidek, Z. (2011). A Framework for the Governance of Information Security in Banking System. *Journal of Information Assurance & Cybersecurity*, 23(8), 1–12. doi:10.5171/2011.726196
- Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, 24(2), 99–104. doi:10.1016/j.cose.2005.02.002
- von Solms, R., & van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security*, 38, 97–102. doi:10.1016/j.cose.2013.04.004
- Von Solms, S. H. (2005). Information Security Governance - Compliance management vs operational management. *Computers & Security*, 24(6), 443–447. doi:10.1016/j.cose.2005.07.003

Information Security Governance in Large Organizations

Waddock, S. A., & Graves, S. B. (1997). The Corporate Social Performance-Financial Performance Link. *Strategic Management Journal*, 18(4), 303–319. doi:10.1002/(SICI)1097-0266(199704)18:4<303::AID-SMJ869>3.0.CO;2-G

Williams, P. (2001). Information Security Governance. *Information Security Technical Report*, 6(3), 60–70. doi:10.1016/S1363-4127(01)00309-0

Williams, P. (2007). Executive and board roles in information security. *Network Security* (Vol. 2007). doi:10.1016/S1353-4858(07)70073-9

APPENDIX 1

Table 7. Governance maturity assessment roadmap

Security Governance Function	AB	Security Practices	Maturity Score	significance Score
Information security governance Strategy and Metrics	SM1	Information Security Strategy and policies	0,93	2
	SM2	Strategic alignment of security	1,25	2,5
	SM3	Communication and Training	1	2
	SM4	People Roles and responsibilities	1,67	2,8
	SM5	Security performance assessment	1,24	2,5
	SM6	Assessment of security budget and investments	2	3
Technical Asset Security Management	AS1	Security architecture	1,67	2,4
	AS2	IT component Security	1,55	2,4
	AS3	Physical infrastructure Security	2,67	3,5
Information Service and Data Security Management	SD1	Incident Management	2	3
	SD2	Ressource Effectiveness	1,5	2
	SD3	Data identification and Classifications	0,93	2
	SD4	Access Management	1,35	2
	SD5	System Acquisition, Development, and Maintenance Security Policy	0,75	1,5
Vulnerability and Risk Management	RM1	Security Threat profiling	1,4	2
	RM2	Security Risk Assessment	1,5	2,5
	RM3	Security Risk Prioritization	0,85	2
	RM4	Security Monitoring	1,65	2,2
Information Security Governance Control/Compliance/Continuity Management	SC1	Compliance Control	0,95	2
	SC2	Security Testing and Auditing	1,8	2,5
	SC3	Business continuity planning	0,5	1,5

APPENDIX 2

Table 8. Governance maturity assessment interview (sample)

Information security governance Strategy and Metrics		Current State	
Information Security Strategy and policies		Answer	Rating
SP1	Is there an information security policy and program in place?	Yes in ad-hoc basis	0,93
	Do the security rules specify a clear definition of tasks, specific roles affecting information security officers?	Yes a small percentage are/do	
	A plan ensures that the review is conducted in response to changes in the baseline of the initial assessment, such as major security incidents, new vulnerabilities, or changes to organizational or technical infrastructure?	Yes there is a standard set	
	Is there a formal contract containing, or referring to all security requirements to ensure compliance with the organization's security policies and standards?	Yes a small percentage are/do	
SP2	Management actively supports the organization's security policy through clear direction, demonstrated commitment, explicit function assignment, and recognition of information security responsibilities?	Yes at least half of them are/do	
	Are risk ratings used to adopt security and insurance required?	No	
	Does the organization know what's required based on risk ratings?	Yes at least half of them are/do	
Strategic Alignment of Security		Answer	Rating
SA1	Does the organization measure the contribution of IT security to its performance?	Yes a small percentage are/do	1,25
	Does the organization defined and managed the role of information security in the face of business and technological change?	Yes but on an ad-hoc basis	
SA2	Are there formal processes in place that emphasize strengthening the partnership relationships between IT Security and Business (e.g. cross-functional teams, training, risk sharing/recognition)?	Yes there is a standard set	
	What is the degree of IT control of security or business changes (implementation of new technology, business process, merger/acquisition)?	Yes, a small percentage are/do	
SA3	What is the degree of perception of IT Security by the organization?	Yes, a small percentage are/do	
	Does the organization periodically use audits to collect and control compliance conformity?	Yes, localized to business areas	
Communication and Training		Answer	Rating
CT1	Have IT staff been given high-level security awareness training?	Yes we do it every few years	1
	Are system security items included with employee orientation?	Yes at least half of them are/do	
CT2	Are those involved and engaged in the IT process, given specific guidance and training on security roles and responsibilities?	Yes at least half of them are/do	
	Are users aware and equipped to comply with IS principles, policies and procedures	Yes a small percentage are/do	
CT3	Is ongoing security education of users planned and managed?	Yes teams write/run their own	
	There is any regular communication process with unit personnel (unit security newsletter/web page)	Yes a small percentage are/do	

continued on following page

Table 8. Continued

People Roles and responsibilities		Answer	Rating
PR1	Do the security rules specify a clear definition of tasks, specific roles affecting information security officers?	Yes we do it every few years	1,67
	Are the roles and responsibilities for the safety of employees, contractors and third-party users defined and documented by the organization's information security policy?	Yes at least half of them are/do	
PR2	Are users, IT Staff and providers gave roles and responsibilities for throughout the organization?	Yes at least half of them are/do	
	Are information security responsibilities allocated to ensure accountability and responsibility for the implementation of IS initiatives?	Yes a small percentage are/do	
PR3	Is security-related guidance centrally controlled and consistently distributed throughout the organization?	Yes teams write/run their own	
	Are responsibilities identified at the unit and at the division or enterprise level?	Yes we did it once	
Security Performance Assessment		Answer	Rating
PA1	Are management oversight performed to ensure security measures in line with business requirements?	Yes we do it every few years	1,24
	Does the organization use any tools or proprietary methods for conducting risk assessments and keeping the IT contingency plans up-to-date?	Yes at least half of them are/do	
PA2	Has a risk assessment been conducted?	Yes at least half of them are/do	
	Is there an overall coordination plan for implementation, including damage assessment, emergency response salvage, etc.?	Yes a small percentage are/do	
PA3	Are reports concerning risk assessments and risk mitigation measures produced regularly?	No	
	Are standard reports concerning performance produced on a regular basis?	Yes we did it once	
Assessment of Security Budget and Investments		Answer	Rating
B11	Does Financial Management for IT Security provide information concerning forecasts for IT service delivery expenditure?	Yes we do it every few years	2
	Does Financial Management of IT security offer information about the actual costs of providing services and resources against planned costs?	Yes at least half of them are/do	
B12	Does Financial Management for IT Security provide information concerning the performance of managing service costs against the financial target?	Yes at least half of them are/do	
	Does Financial Management for IT Security provide information concerning actions necessary to achieve financial targets?	Yes a small percentage are/do	
B13	Does Financial Management for IT Security provide information concerning the analysis of deviations from plans?	Yes teams write/run their own	
	Does Financial Management for IT Security provide information concerning the current charging policies & IT Accounting methods?	Yes we did it once	

Chapter 9

Information Security Policy in Large Public Organizations: A Case Study Through ISO 27002

ABSTRACT

The aim of this chapter is to study the success factors of the ISO 27002 framework related to the implementation of information security in organizations, with particular emphasis on the different maturity controls of ISO 27002 in the implementation of information security policies in organizations. The purpose of this chapter is to investigate what controls are commonly used and how they are selected to the implementation of an information security in large public organizations in Middle East and North Africa (MENA) through ISO27002, with a specific focus on practical framework for the implementation of an effective information security policy through ISO27002. The finding will help organizations to assess organizations to implement an effective information security policy.

INTRODUCTION

Information Systems (IS) are today an integral part of the functioning of public administrations and bodies, the activity of businesses and the way of life of citizens. The security of these information systems has become a major issue for all public or private sectors, which would be very strongly affected in the event of serious malfunctions (T. R Peltier, 2016).

DOI: 10.4018/978-1-5225-7826-0.ch009

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Information security policy is the general term used to describe any document that transmits an element of the security program in order to ensure compliance with the organization's security goals and objectives. Since this definition covers a wide range of security policy documents, it is useful to describe the various types of information security policies that an organization may use. The terms used below to describe these types of information security policies are generally used in the information security industry and will be used consistently throughout this chapter (Ifinedo, 2014). However, it is not unusual for a government organization or agency to have different names for the same types of information security policies. For example, in many organizations and certainly in government departments, the word "policy" is closely associated with laws and regulations (Rees, Bandyopadhyay, & Spafford, 2003). In these cases, a limited number of individuals (e.g., the legislature) have the power to create a policy, so that an information security policy is generally referred to by other names such as "information security statement", or "information security document" or other terms avoiding the use of the word "policy". The term used by an organization to describe these documents is irrelevant. The overall organization and completeness of these documents are important (Hong, Chi, Chao, & Tang, 2006).

The security policy is primarily implemented as a means of communication with system users and administrators, issues that must be taken into account when security decisions are made. It defines the explicit expectations and responsibilities of users and administrators, and allows both groups to know what to expect from each other (K. Knapp, Morris, E. Marshall, & Byrd, 2009). It should explain why certain decisions have been made and why they are important, to help all users understand how the policy is designed to benefit them (Flowerday & Tuyikeze, 2016).

The security policy should specifically state the types of data that are considered important enough to warrant protection. This would include user's personal files in the form of programs, text documents like a thesis or an email message, as well as system-specific configuration files (Yassine, Maleh; Abdelkebir, Sahid; Abdellah, 2017). This helps to allow users to better understand why security measures are in place, and why certain insecure services have been restricted.

A password policy is already in place, however it should most definitely be mentioned in the security policy. This is one of many things the user could do to help keep the system secure, but is probably one of the most important. Other ways that a user could contribute to system security would be properly

managing their file and directory permissions or using other software that was designed with the security conscious person in mind (K. Knapp et al., 2009).

Should a security incident occur, the security policy should state who is responsible for restoring the system to a secure state, as well as any procedures that should be followed throughout the course of the repair. If the person in charge of system security detects a break in, who should be notified and what should be done with the compromised machine? Issues like these must be addressed in order to ensure that firstly any disrupted services are restored in a timely manner and secondly so that proof of the incident can be obtained should the legal need arise (Maleh, 2018). The source of the security breach should be determined and fixed so the incident doesn't repeat itself and once the problem has been properly documented, the system administration team should be made aware of what happened.

The Information Systems Security Policy (ISSP) reflects the expectations and requirements of the Executive Management with regard to the Information System (Canavan, 2003; Höne & Eloff, 2002b; Canavan, 2003). It must take into account at least the needs in terms of availability, confidentiality and integrity of applications and data used and transiting on networks and systems. It consolidates a set of technical, organizational, legal and human security rules and principles to ensure an efficient and uniform level of security (Fomin, 2008). The ISSP is the counterpart of the Information Systems Master Plan for security. It can lead to an ISSP action plan that prioritizes projects to meet ISSP objectives. The objectives of the Information Systems Security Policy (ISSP) are described in Figure 1.

There are several standards and best practice guidelines to assist organizations in implementing an information systems security policy such as ISO 27000, ISACA, NIST, etc. ISO 27001 (ISECT, 2012) is an international standard that is part of the ISO 27000 family of standards (Von Solms, 2005). It refers to a set of standards relating to the information security management system. The ISO 27001 standard is a British standard that came into being in October 2005, succeeding the BS 7799-2 standard. It describes the requirements for the implementation of an Information Security Management System as shown in Figure 1. This standard allows companies to choose security measures to ensure the protection of sensitive assets within a well-defined perimeter by implementing a systematic and proactive approach to security risk management.

Figure 1. Information system security policy objectives

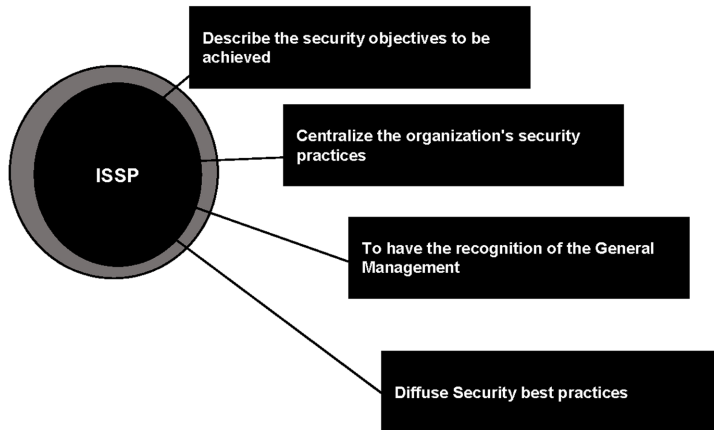
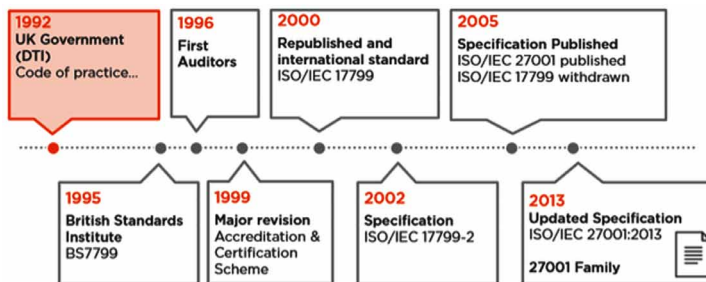


Figure 2. A brief history of ISO/IEC 27001



Best practice guides such as ISO 27000, COBIT, ISACA do not provide the practical framework for implementing an IS security policy (Höne & Eloff, 2002a). The objective is to guide organizations in their approach to implementing an IS Security Policy through a practical guide to implementing an IS Security Policy.

Problem Statement

Many prescriptive approaches to ISO 27002 already exist, for example ISO 27003, which is the official standard with guidelines for ISO 27001 (Talib, M. A., El Barachi, M., Khelifi, A., & Ormandjieva, 2012). Several steps to implement the management framework provided in ISO 27001, called the information security management system ISMS, are presented. However,

a practical methodology for implementing an information security policy does not exist.

Many organizations do not have the resources or expertise to conduct a risk analysis and implement an ISMS (Mintzberg, H., Lampel, J., & Quinn, 2003). Therefore, they could now know what aspects of security might be relevant to them. Instead of doing a comprehensive risk analysis, an organization could also look to its peers. What are they doing? Although it is not as good to follow your peers as it is to do an extensive risk analysis, it is certainly better than setting up controls for no reason.

Modern times require different approaches to problems. Nowadays, mobile phones and tablets are common products. Employees are supposed to work everywhere. Information is quickly shared via social media. How do companies manage these new issues - what controls do they put in place and how do they select them?

To date, there was no literature on practical research using ISO 27000, using Google Scholar and SCOPUS. Almost all results had a very limited number of references. However, some were still useful. The following paragraphs describe the documentation used for the research.

There are very few scientific papers on ISO 27002, and none found that research practice uses ISO 27002 controls as described in the background section. This chapter can be considered exploratory: The data collected in this research may well be used to formulate hypotheses for other research projects.

Research Question/Approach

The research question in this work is: What relevant ISO 27002 controls and good practices do corporate information security managers choose to implement, and why are they chosen?

The approach taken in this research is qualitative research, using interviews with experts. Expert interviews are a good way to explore an area of research. Experts often know a lot about the research topic. By talking to several of them, it is possible to know whether there is a consensus or whether there is still much debate on certain subjects. Both results could be used in future research.

Unlike quantitative research, qualitative research is used to focus more on “why” and “how” questions. As a result, qualitative research generally takes smaller, but more focused samples than quantitative research. Qualitative research often does not have a clear hypothesis in advance. Instead, we need an

open question. The selection is not made by statistical chance, but according to what is available. When interviewing information security officials, the objective is to get an overview of the controls they choose and why they have been chosen over others.

Purpose

As there is very little scientific literature on the practical use of ISO 27002, this research can be used as exploratory research. The purpose of this chapter is to investigate what controls are commonly used and how they are selected to the implementation of an information security in large public organizations in Middle East and North Africa MENA through ISO27002 (Calder, A., & Watkins, 2010), with a specific focus on practical framework for the implementation of an effective information security policy through ISO27002 (Calder, A., & Watkins, 2010).

BACKGROUND

The business policy has been conceptualized as a form of strategic management (Mintzberg, 1983). Two perspectives make up the way in which strategy is made: deliberate formulation and emergent formation (Mintzberg, 1983). The classical approach advocated by Quinn is the approach to strategy grounded in the military strategy used for thousands of years. This type of strategy advocates the use of deliberate plans to win battles and wars. Noted historical figures in the area of military strategies, such as Sun Tzu, Napoleon, Lenin, and Machiavelli have contributed to advancing the classical strategy to its modern form. Rees et al. (2003) stepped away from this rigid approach to business strategy and policy by advocating an emergent approach. In this, an organization's realized strategy is a combination of the organizations deliberate strategy with the evolving emergent strategy. This emergent strategy is identified by a stream of actions which can represent a pattern.

These two perspectives of strategic management can be used to investigate the research behind IS security policy. One stream is grounded in the classical approach while the other in the emergent approach. The following section will utilize each of these perspectives in examining the literature behind IS security policy.

From the classical, planned strategic perspective, research has aimed to provide information security professionals and top management a framework through which useable security strategy and policy for applications can be created and maintained in line with the standard information technology life cycle (Glasgow, Macewen, & Panangaden, 1992). This framework was cyclical in nature and consisted of four stages, plan, access, operate, and deliver. At the theoretical level, Kühnhauser, (1999) created a formal framework for specifying security policies. This framework, called Security Logic, defines what a subject knows, what information a subject has permission to know, and what information a subject is obligated to know. The paper presented this via a logical approach based on modal logic formalism.

Continuing with the classical perspective, Kühnhauser, (1999) expounded on how to rationally plan out the multi-policy system. These are defined as systems that support a multitude of independent security domains in which an individual IS Security Policy is enforced on the applications. Joshi, Ghafoor, Aref, and Spafford (2001) performed a logical analysis to introduce a formal model of policy groups. Research has also examined the issue of multi-policy systems by investigating the emerging “digital government” (K. J. Knapp, Marshall, Rainer, & Ford, 2007). A sequence of solutions to the issues of multi-domain environments are presented including ad hoc approaches, formal approaches, model-based methods, agent-based methods, architectural methods, and the database federation approach. Policy enforcement however does not highly correlate with policy effectiveness (Baskerville & Siponen, 2002).

The classical perspective has also witnessed a call for a security meta-policy (Willison, 2002). It is noted that existing IS Security Policy approaches do not pay much attention to policy formulation itself. In other words, the actual creation of the policy is done in an ad hoc manner. Calling for a meta-policy implies that the way to the best strategy or policy is through concise rational planning.

On the emergent side of the strategic paradigm, researchers have examined how problems are dealt with after the creation of an IS security policy. It has been noted that 52% of all logistical and physical security breaches arose from the activities of personnel within the organization (Ahmad & Ruighaver, 2003). Research has sought to determine the most optimal control method to handle these breaches. IS Security Policy formally defines security requirements, outline the main security objectives, and allocate responsibilities. To maximize the probability of compliance, the enlightenment of staff to their responsibilities as outlined in the IS Security Policy is one potential solution.

Also from the emergent perspective, there has been a call for the improvement of audit management technology to allow administrators to configure the software to reflect the security needs of an organization as defined in the IS Security Policy. This demonstrates a dynamic approach to the policy in that it can be reactive to how an audit trail affects an Information System. Changing the configuration from the status quo bottom-up approach to a policy-centric top-down approach would help the configuration more closely match an organization's security goals (Coyne & Kluksdahl, 1994).

While not explicitly approaching the issue from an emergent perspective, Coyne and Kluksdahl (1994) examination of a failed IS Security Policy implementation demonstrates an analysis from an emergent perspective. The implication resides in how the implementers could have adapted to how the actual scenario was different from the rational plan. They found that compliance-based approaches are more prone to failure than risk-based approaches. A de-facto compliance-based policy led to the reaction of all security-related matters being adversarial in nature (Walsham, 1993).

This research was conducted via an interpretive case study in the Information Technology Department of a large state University in the south-eastern portion of the United States. The interpretive tradition perceives that the knowledge of reality is a social construction by human actors (Howcroft, 2005). In contrast to the assumptions of positivist science, this knowledge of reality applies equally to researchers and leads to the perception that there is no objective reality which can be discovered by researchers. This perspective is also described whereby "interpretive research provides in-depth insights into social, cultural and historical contexts within which particular events and actions are described and interpreted as grounded in the authentic experiences of the people studied" (Reich & Benbasat, 2000).

Approximately 45 employees worked for the department under study. Of these, 20 participated in the interviews. The subjects that did participate were the stakeholders involved in the formulation and implementation of the IS Security Policy. They included the Chief Information Officer, Security Officer, and a group of operational level employees who were members of a Security Planning Team (SPT). The members of SPT included systems analysts, web developers, a database administrator, two school administrators, and three faculty members. The employees within the department who did not participate in the study included those that were not stakeholders in the IS Security policy formulation and implementation process.

The interviews were grounded by the previously discussed conceptual framework. Though the interview questions were grounded in the theoretical framework, they were conducted in a semi-structured manner. Many IS researchers have utilized semi-structured interviewing techniques such as (Walsham, 1993). The semi-structured nature of the interview questions helped facilitate affective aspects. As discussed in the framework, affective aspects refer to subjective value judgments. Immediately after each of the interviews, the investigator debriefed. This process of immediate “debriefing” helped to clarify the researcher’s interpretations and deepen his level of understanding (Walsham, 1993).

Besides gathering data, the interviews served as subject recruitment opportunities. The process of building the network of interviewees was done in a “referral” manner. This means that the interviewees themselves will point the researcher to the next best contacts in which to continue the interview process. The point of saturation became apparent when the same names began to appear. It was at this point that the totality of who the stakeholders were that were involved in the IS Security policy process became clear (Walsham, 1993).

Once the interview process was complete, the data was interpreted by the researcher (Fomin, 2008). This process involved a systematic analysis and categorization of the data by emergent themes that the researcher identified. These themes were not known a priori but emerged as the data was categorized by thematic principles. These thematic principles, which included such topics as security awareness, deterrence, and resistance, emerged in part from existing themes in the security literature and by the data gathered in the course of the study.

Gikas (2010) is trying to find the reasons for the low adoption of the international ISO/IEC 2700 standard on information security management. The author compares ISO/IEC 27001 with the other two widely applied management system standards - ISO 9001 for quality management and ISO 14001 for environmental management - and shows that in addition to low adoption rates, ISO/IEC 27001 has attracted much less academic interest, as evidenced by the number of scholarly publications on the subject. The author compares the reasons for the application of ISO/IEC 27001 with those of ISO 9001 and concludes by listing possible factors and obstacles for the dissemination of standards and suggesting a roadmap for future research on the subject.

Gillies (2011) discusses two pieces of legislation (HIPAA and FISMA) that focus on information security for US government agencies and two private sector standards (PCI-DSS and ISO 27000) that address the information security needs of a broader range of institutional users of information technology (IT). It will provide a brief description of the four entities, a high-level comparison of suggested and/or prescribed guidelines to identify gaps and overlaps, and suggest a possible threshold model that could incorporate safety parameters that meet the requirements of the four entities.

ISO, I., & Std (2005) is looking at global adoption of the ISO27000 series of standards and comparing them with ISO9000 and ISO14000 adoption rates. They compare the barriers to the adoption of different standards. Adoption of ISO27001 has been slower than ISO9001 and ISO14001 management system standards, with about half of ISO14001 certifications. In response to the questions raised in this analysis, the paper examines how a maturity model approach can be used to help overcome these barriers, particularly in small businesses. The 2008 survey of ISO27001 certified companies found that 50% of the certified organizations that responded had fewer than 200 employees and therefore fell into the SME category. The framework used the ISO code of practice 27002 to define the elements that should be taken into account in ISMS. Each element is then developed through a maturity model life cycle to develop processes to the point where an ISO27001 compliant ISMS can be implemented.

The ISO/IEC 2700x Family

Several standards, methods and repositories of good practices in information systems security are available. They constitute methodological guides as well as the means to guarantee a coherent security approach.

ISO has undertaken a major effort to streamline existing work, resulting in the ISO/IEC 27000 series of standards. This number corresponds to the reservation of a series of safety standards. To date, only standards 27000, 27001, 27002 and 27006 are published. Some are mandatory to obtain certification, others are mere guides:

- ISO/IEC 27000 presents the vocabulary and definitions of the security field, applicable to each of the standards;
- ISO/IEC 27001 describes the information systems security management policy within a company that serves as a reference for certification;
- ISO/IEC 27002 is the good practice guide for IS security;

Information Security Policy in Large Public Organizations

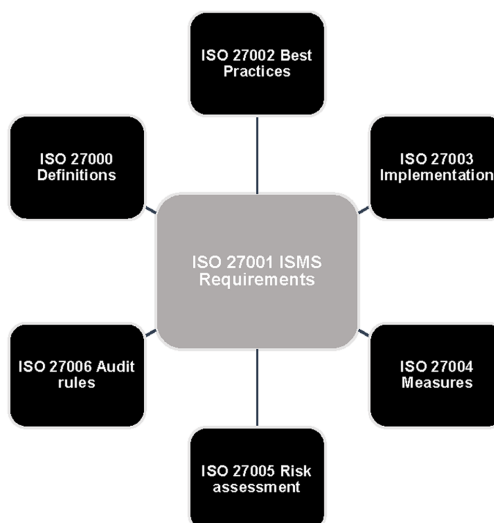
- ISO/IEC 27003 is intended to be an implementation guide;
- ISO/IEC 27004 will be a new standard for steering indicators and measurements in the field of IS security;
- ISO/IEC 27005 will be a new standard on risk management for IS security;
- ISO/IEC 27006 summarizes the requirements applicable to external auditors in their ISO 27001 certification assignment.

As shown in Figure 3, ISO/IEC 27001 is the center of gravity of the Information security management system ISMS referential.

ISO/IEC 27001

The ISO/IEC 27001 standard, published in November 2005, defines the IS security management policy within a company (Johnson, 2014). It is derived from the BS 7799-2:1999 specification (Specification for Information Security Management Systems) which defines the requirements to be met to create an ISMS (PRGL, 2011). It specifies in the annex certain safety controls, taken from the ISO/IEC 17799 standard, the implementation of which is mandatory. ISO 27001 comprises six process areas.

Figure 3. The ISO 2700x series



- Define an information security policy.
- Define the scope of the information security management system.
- Conduct a safety risk assessment.
- Manage identified risks.
- Select and implement controls.
- Prepare a SoA (Statement of Applicability).

ISO 27001 specifies the processes that enable a company to build, manage and maintain an information security management system. It integrates the process approach and the PDCA (Plan-Do-Check-Act) cycle of continuous improvement already contained in ISO 9001 and ISO 14001 standards:

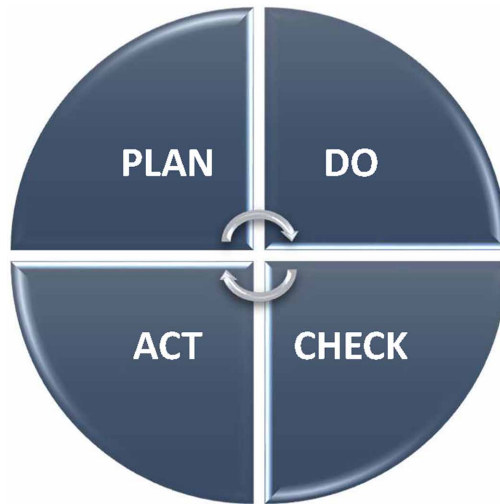
- **Plan:** Organize the implementation of the information security management system;
- **Do:** Set up and operate the system;
- **Check:** Monitor system effectiveness through internal audits and risk assessments;
- **Act:** Improve the system through appropriate corrective and preventive actions, maintain it through communication and training actions.

In terms of security, the improvement loop is synonymous with a risk reduction loop. In practice, procedures should be put in place for:

- Quickly detect processing errors;
- Immediately identify any non-compliance with safety rules and organize the immediate reporting of incidents;
- Verify that all safety-related tasks are actually performed, whether by men or automatons;
- Identify the actions to be taken to correct non-compliance with safety rules.

As regards control, regular reviews of the effectiveness of the system should be carried out on the basis of audit results, incident reports and suggestions and comments received from the parties concerned. On the other hand, acceptable residual risk levels must be continuously reviewed and adapted in the light of organizational, technological, legal and regulatory developments or public opinion.

Figure 4. PDCA cycle



Measurement requirements are explicitly contained in the standard in the form of risk assessments, audits, incident data collection and non-compliance. However, the standard lacks metrics that would make it easier to compare certified entities with a single repository.

ISO/IEC 27002:2005 (Revised by ISO/IEC 27002:2013)

ISO/IEC 27002:2005 is another generic standard that can be applied to health information systems to ensure security. It establishes general principles and guidelines for effective initialization, implementation, maintenance and improvement of information security management. The objectives outlined therein provide general guidance on the commonly accepted goals of information security management. Thus any organization seeking to adopt a comprehensive information security management program or improve its existing information security practices can use the standard. The ISO standard asserts that information can be protected using a wide variety of controls. Such controls include hardware and software functions, procedures, policies, processes and organizational structures. Organizations including healthcare organizations, must develop, implement, monitor, evaluate and improve these types of security controls (PRGL, 2011).

ISO/IEC 27002:2005

ISO/IEC 27002 2005 is entitled Information technology - Security techniques - Code of practice for information security management. It is published by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

ISO/IEC 27002:2005 was developed from BS7799, a British standard that was published in the 1990s. ISO/IEC adopted this standard as ISO/IEC 17799:2000 in December 2000. In June 2005, the standard was revised and officially published as ISO/IEC 17799:2005. On July 1, 2007, it was renumbered ISO/IEC 27002:2005 to align with the other ISO/IEC 27000-series standards (ISO/IEC, 2013). On the other hand, ISO/IEC 27002:2005 has been revised by ISO/IEC 27002:2013 (ISECT, 2012).

In this research, ISO 27002 serves as the framework for measuring information security in organizations. It is surprisingly well suited to this work, as the idea behind ISO 27002 is to have a list of controls that should be able to mitigate all possible information security risks.

ISO/IEC 27002:2005

The thirty-nine main security categories of the standard are specified under eleven security control clauses. Each main security category contains one control objective stating what is to be achieved. In addition, one or more controls are specified to help achieve the control objective. The standard also has one introductory clause that discusses risk assessment and treatment. The control clauses include:

1. Risk assessment and treatment
2. Security policy
3. Organization of information security
4. Asset management
5. Human resources security
6. Physical and environmental security
7. Communications and operations management
8. Access control
9. Information systems acquisition, development and maintenance
10. Information security incident management
11. Business continuity management
12. Compliance

Although ISO/IEC recommends a complete consideration of the practices, organizations do not have to implement every recommended security practice stated therein. The important thing is to know what works best for the unique information security risks and requirements (ISO/IEC, 2013).

ISO / IEC 27001: 2013 now contains 114 controls for 14 domain areas as shown in Table 1 (ISO/IEC, 2013).

Information Security Policies

Objectives

To establish an Information Systems Security Policy published, regularly updated and supported by general management, in order to provide information security guidance in line with business requirements and regulations in force.

The ISSP centralizes the organization's information protection strategy. It is validated by the COSI and approved by the General Management and is available to all the organization's agents and transmitted to the third parties concerned.

Table 1. ISO / IEC 27001: 2013 controls and domains

#	Domain	Number of Controls
1	Information Security Policies	2
2	Organization of Information Security	7
3	Human Resource Security	6
4	Asset Management	10
5	Access Control	14
6	Cryptography	2
7	Physical & Environmental Security	15
8	Operations Security	14
9	Communications Security	7
10	System Acquisition, Development & Maintenance	13
11	Supplier Relationships	5
12	Information Security Incident Management	7
13	Information Security Aspects of Business Continuity	4
14	Compliance	8

Organization of Information Security

Objectives

To manage, monitor and guarantee the security of information within the organization in a transversal way, and to define the responsibilities and roles of the various security actors.

The organization of information security clause addresses the need to define and allocate the necessary roles and responsibilities for information security management processes and activities. This includes controls related to the definition of information security roles and responsibilities, segregation of duties, contact with authorities, contact with special interest groups, information security in project management and mobile devices and teleworking.

Human Resource Security

Objectives

To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. To ensure that employees and contractors are aware of and fulfill their information security responsibilities. And to protect the organization's interests as part of the process of changing or terminating employment.

The Human Resource Security clause addresses the required controls for processes related to staff recruiting, their job during employment and after the termination of their contracts. These considerations should include information security coordination, allocation of information security responsibilities, authorization processes for information processing facilities, confidentiality agreements, contact with authorities, contact with special interest groups, independent review of information security, identification of risks related to external parties, addressing security when dealing with customers, addressing security on contractors' agreements, etc.

Asset Management

Objectives

To identify, inventory and classify all assets required for information management. For each of them, a person in charge must be identified. The latter is responsible for enforcing the security policy for its assets.

The asset management clause addresses the responsibilities that need to be defined and assigned for asset management processes and procedures. The owner of the assets and other parties involved in this issue should be identified to be held responsible for the security of the assets, including classification, labeling and information processing; and the information processing facilities should be identified and maintained. In addition, this clause addresses the control of removable media management, media disposal and physical media transfer.

Access Control

Objectives

To ensure that users are aware of security responsibilities. To reduce the risk of accidents, errors and/or malicious acts by integrating safety principles into human resources management, from recruitment to the end of the collaboration

The access control clause addresses the requirements for controlling access to information assets and information processing facilities. Controls focus on protection against accidental damage or loss, overheating, threats, etc. This requires documented control policies and procedures, registration, removal and review of user access rights, including here physical access, access to the network and control of privileged utilities, and restriction of access to program source code.

Cryptography

Objectives

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

The Cryptography clause addresses policies on cryptographic controls for protection of information to ensure proper and effective use of cryptography in order to protect the confidentiality, authenticity, integrity, non-repudiation and authentication of the information. It also includes the need for digital signatures and message authentication codes, and cryptographic key management.

Physical and Environmental Security

Objectives

To ensure the protection and availability of sensitive equipment. To ensure that only authorized persons have access to the organization's buildings, technical and archive premises and that accesses are traced.

The physical and environmental security clause addresses the need to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

Operations Security

Objectives

To ensure correct and secure operations of information processing facilities. To ensure that information and information processing facilities are protected against malware. To protect against loss of data. To record events and generate evidence. To ensure the integrity of operational systems. To prevent exploitation of technical vulnerabilities. To minimize the impact of audit activities on operational systems.

The Operations security clause addresses the organization's ability to ensure correct and secure operations. The controls cover the need for operational procedures and responsibilities, protection from malware, backup, logging and monitoring, control of operational software, technical vulnerability management, information systems audit considerations.

Communication Security

Objectives

To ensure the protection of information in networks and its supporting information processing facilities. To maintain the security of information transferred within an organization and with any external entity.

The communications security clause addresses the organization's ability to protect information in systems and applications of supporting networks and information processing facilities. Controls cover information security in connected networks and services against unauthorized access, transfer policies and procedures, secure transfer of business information between the organization and external parties, information involved in e-mail, the need for confidentiality or non-disclosure agreements.

System Acquisition, Development and Maintenance

Objectives

To guarantee security management throughout the lifecycle of Information Systems. To reduce the risks associated with exploiting technical and application vulnerabilities.

The System Acquisition, Development and Maintenance clause covers controls for identifying, analyzing and specifying information security requirements, securing application services in development and support processes, technical review restrictions on changes to software packages, secure system engineering principles, secure development environment, outsourced development, system security testing, system acceptance testing and test data protection.

Supplier Relationships

Objectives

To ensure protection of the organization's assets that is accessible by suppliers. To maintain an agreed level of information security and service delivery in line with supplier agreements.

The Supplier Relationships clause addresses controls for supplier's relationship issues, including here information security policies and procedures, addressing security within supplier agreements, communication and awareness about technology supply chain and service delivery management.

Information Security Incident Management

Objective

To ensure a consistent and effective policy for the management of information security incidents. To guarantee the reporting of security events and vulnerabilities. To identify indicators and report on security incidents.

The information security incident management clause covers controls over responsibilities and procedures, reporting information and security weaknesses, assessing and deciding on information security events, responding to information security incidents, learning from information security incidents, and gathering evidence.

Information Security Aspects of Business Continuity Management

Objectives

After a minor incident (equipment failure), provide computer backup according to business needs. After a major incident affecting an entire engine room, ensure continuity of IT activity for sensitive assets as quickly as possible and according to business needs.

The business continuity management clause addresses the organization's ability to counter normal business interruptions, including the availability of information processing facilities, verify, review and assess information security continuity, implement information security continuity and plan information security continuity.

Compliance

Objectives

To avoid any violation of intellectual property, legal, regulatory and contractual provisions and security requirements of the organization.

The compliance clause addresses the organization's ability to comply with regulatory, statutory, contractual and security requirements, including identification of applicable laws and contractual requirements, intellectual property rights, record protection, confidentiality and protection of personally identifiable information, regulation of cryptographic controls, independent review of information security, compliance with security policies and standards, and review of technical compliance.

Other ISO 27000 Standards

In addition to ISO 27001 and 27002, there are several other ISO standards in the 27000 range. These other standards guide and support ISO 27001/27002 for both organizations and auditors.

ISO 27003

ISO 27003 is used as the implementation standard for ISO 27001. This standard is intended to obtain management approval, define CMSS, conduct an organizational analysis and a risk analysis.

ISO 27004

ISO 27004 is a standard that helps measure the effectiveness of ISMS. ISO 27004 includes the following chapters:

- Overview of Information Security Measurement; Management Responsibilities;
- Measurement and measurement development;
- Measurement operation;
- Data analysis and reporting on measurement results;
- Evaluation and improvement of the information security measurement program.

ISO 27005

ISO 27005 is a standard that provides guidance for the implementation of ISO 27001. ISO 27005's approach begins by setting the context - defining the scope (primary processes and related assets) and boundaries of the organization. When defining the scope, a risk analysis will be carried out. Risk analysis consists of identifying the assets and the threats they face. In addition, the impact of a successful exploitation of a certain threat must be analyzed. When this is done, for each threat, an estimate of the likelihood that the threat will be successfully exploited will be multiplied by the costs of the impact of that exploitation. Based on this list, each risk should be mitigated through the implementation of controls, risk acceptance, risk avoidance or risk transfer.

ISO 27006 and Certification

An organization can be certified ISO 27001. This can only be done by accredited auditors. The organization can only be certified if the ISMS and a number of controls are properly implemented. ISO 27002 defines how an auditor can evaluate an organization in order to accredit it. ISO 27002 defines two steps for the accreditation of an organization.

RESEARCH METHODOLOGY

Data Collect

As part of this research, MENA large organizations experts are interviewed. These experts hold the title of security officer, or what most closely resembles their organization. We chose the large public sector organizations because there are interesting problems specific to this sector. For example, government organizations usually possess a lot of privacy-sensitive data - e.g., information about citizens. In addition, it appears that data leaks from public bodies are often well exposed in the media.

For the first round. We mailed a letter with details of the research content, what they would be asked for and what their own benefits were, before sending the final question, which is an optimized version of the ISO 27002 questionnaire presented in the Appendix (Table 4). A total of 20 organizations

were selected, 6 organizations agreed to give us interviews to answer our questions, i.e. 30%, a percentage too credible for this research.

In the second round, we validate the first study result with a qualitative methodology through a case study in a large public organization in Morocco.

As we conducted interviews by e-mail, we did not need to go to the locations of the interviewees. Therefore, the interviews did not require travel expenses. When participants sent me answers that we could not understand, we could then ask them to give me more details or explanations on previous comments. The email interviews allowed us to interview several participants at the same time. They were also easy to transcribe. At the same time, there was a lack of richness in the responses we received from participants. It was also not easy for participants to get clarification on the meaning of the questions, so we sent them a brief explanation of the theories by email. These explanations would improve their possibilities if they gave appropriate answers. Table 2 shows the summary of key attributes of participating organizations.

Data Analysis

For each interview, a report was written. The size was limited to about one page. The following section contains the reports from each interview. For reasons of anonymity, organizations are indicated by alphabets from A to F. The questionnaire results for each organization are presented in the next section. For each organization, the scores for each sub-theme are displayed.

The quotation is based on ISO/IEC 27002:2013 (Thomas R. Peltier, 2013). Each question is waiting for an answer in the form according to the maturity model described in Table 3.

Table 2. Summary of key attributes of MENA organizations

Organizations	A	B	C	D	E	F
No of employees	1125	2400	7000	12000	2400	1700
No of IT staff	80	190	220	420	44	35
No of IT Security staff	5	12	9	10	3	5
Government (Gov.)/ Multinational (multi.)	Gov.	Gov.	Gov.	Gov.	Gov.	Gov.
ISO 27002 Version	V4	V4	V4	v V5	V5	V4
Certified ISO 27002 Lead auditor staff	6%	5%	3%	3%	7%	0%

Table 3. The maturity level model

Value	Short Name	Description	Details
0	Non-Existant	Nonexistent; Process does not exist or is not applied	Non-existent—Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.
1	Initial / Ad-Hoc	Initial / Ad-Hoc; Process are adhoc and disorganized	Initial/Ad Hoc—There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.
2	Repeatable	Repeatable but Intuitive; Processes follow a regular pattern	Repeatable but Intuitive—Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
3	Defined	Defined; Processes are documented and communicated	Defined Process—Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
4	Managed and Measured	Managed and Measured; Processes are monitored and measured	Managed and Measurable—Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5	Optimized	Optimized; Good practices are followed and automated	Optimised—Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

RESULTS AND DISCUSSION

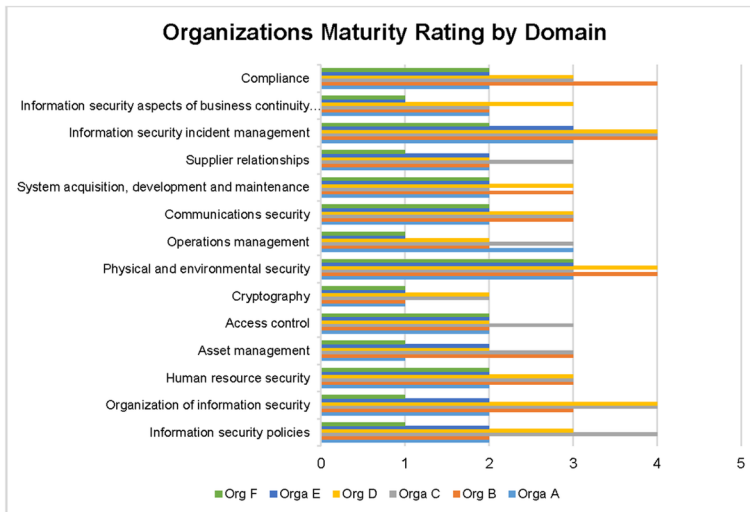
The following Figure 5 provides an overview of how the six organizations ranked for each of the sub-themes.

For organization A, E and F there is no specific security agent. However, one group of people is responsible for information security. The Information Security Policy was created in 2012 and is approved by management. However, the IT security policy is not signed by management.

For these organizations, the most important controls are those related to information security, for example high-level policies, risk assessment. This means that the following three documents must exist and be signed by management:

Information Security Policy in Large Public Organizations

Figure 5. Organizations maturity rating through ISO/IEC 27001:2013



**For a more accurate representation see the electronic version.*

- Information Security Policy Information Technology Policy
- Classification of information sources

Security awareness should also be emphasized. In these organizations, awareness training is organized so that employees are knowingly incompetent in information security, rather than unconsciously incompetent.

Management should become more aware of safety issues themselves, in order to play an exemplary role vis-à-vis other employees. An example of this is: According to the information security policy, identification badges must be displayed at all times. Management does not do it itself.

For Organization E. One of the major problems within the organization is that information security is not an integral part of the organization, but something that is considered an IT problem. This results in several problems for the security guard, for example:

- Lack of management commitment - information security policy has not been approved/signed by management.
- Not all information security issues are technical. For example, in the past, employees did not need a non-disclosure agreement. This situation changed in the spring of 2014, requiring all new employees to sign a non-disclosure agreement.

- There is no confidentiality classification for the information.
- There is no list of processes within the organization.
- There are several courses for employees, for example a LinkedIn course or an Office course.

However, information security is little or not taken into account in these courses. Employees know little about how their actions (online) could harm the organization's image.

All contracts with third parties contain information security clauses. This includes cleaners. An outside company disposes of used paper and hard drives.

There are employment procedures, both for new employees and for dismissals. However, these procedures are not always followed correctly - employees only get more access rights and almost never less, even if their work no longer requires it. It is possible for employees to work from home. Authentication works with an SMS token, which gives the user access similar to what is possible in the office.

For organization F. For the moment, there is still no information security policy. However, interviews were conducted with experts within the organization to develop a list of ISO 27002 controls that should be implemented.

The systems used are shared with other organizations in a shared service center. This center also includes a service desk for incidents. For high priority incidents, a process is in place that includes management and impacts analysis. Physical access is regulated by the use of tokens, where access is distributed according to need. Utility offices have emergency buttons that can be used in the event of disturbance in freely accessible areas. At night, the inner courtyard is locked with fences by the security team.

The organization has undergone intrusion tests, for example using a mystery guest. A mystery guest is a person hired by the organization to pose as a stranger trying to access critical information. This mystery guest made a video about how to get in. This video was shown to management to raise awareness.

It is possible to bring a mobile phone or a tablet computer. There are three different wireless networks - a public network, one for guests and one for employees. These use a ticket system, which allows only one device for a certain time. Thereafter, a new ticket must be requested.

Basically, information security is always a secondary issue, and the level of maturity switches between level 1 (ad-hoc) and 2 (repeatable). Efforts must be made to complete level 3 (defined) and 4 (managed), especially in

the areas of asset management, operation management, supplier relationships, business continuity and compliance.

For organizations B, C and D. Within these organizations, ISO 27002 is used as a guideline for information security. Currently, a baseline is applied across these organizations.

On third parties: Paper waste is disposed of by a company specializing in organization C and D. For as much software as possible, a SaaS solution is used. However, change management is always done within the organization. Backups are performed regularly and tested. Physical security has three different zones: Public areas, employee areas and specific areas, such as server rooms. Organizations support telework through a VPN virtual private network.

For organizations C and D. In these two organizations, a difference is made between the information security policy and the information security plan. The policy is higher than the plan. The plan is based on ISO 27002 controls. Controls are selected using a risk analysis: A matrix of estimated risks and impacts is established and serves as the basis for the selection of controls.

Employees of these organizations were not sworn in, with the exception of temporary staff. Instead, they must sign a non-disclosure agreement. Employees are informed of information security through intranet bulletins, but there is no policy in place for security awareness training.

For third parties, for example application hosting, information security clauses are either included in the terms of service or included in the contract.

A third party takes care of all the equipment that needs to be disposed of, including paper, old computers, printers, etc. When it comes to new applications, ready-to-use solutions are preferred to custom software. If necessary, they can be modified to meet additional needs. For large requests, a tendering procedure is organised. There is a formal change management process, which has improved considerably in recent years.

There are several networks within this organization, and they are physically or virtually separate. For example, there is a network on which employees are connected, one for servers, a public wireless network, a wireless network for employees. Both can be used for mobile devices and are therefore not connected to other networks.

Each week, a list of terminated employees is generated and used to ensure that these employees no longer have access to the applications. There is an employee transfer procedure. However, since a transfer may take some time during which the employee may still need their former access rights, it is more difficult than hiring and termination.

It is possible to work from home. A virtual office system is used, giving a virtual workplace at home. In the future, the computers in the office will use the same system. In the office, all office spaces are flexible: no fixed rooms for employees.

For incidents, a form exists on the intranet for organization E. Depending on the incident, it is assigned either to facilities management or to IT. There, priority is given, depending on the impact of the incident. There is an escalation procedure: the more important an incident is, the more important the follow-up of an incident is. This may be management or a subsequent evaluation.

In general, the 3 organizations are at level 3 (defined). At least efforts must be made in areas such as cryptography and Information security aspects of business continuity management.

CASE STUDY

A qualitative methodology was used and semi-structured interviews were conducted in the study (Creswell, J. W., & Creswell, 2017). An interview guide was developed containing open questions. The interview questions were based on ISO 27002. The interview guide is presented in the Appendix (Table 4). We organized a meeting with the interviewees in order to explain the control objectives and we also sent a short explanation of the theories by email (Burns, 2010). Accordingly, those explanations would enhance their possibility if giving adequate answers. The next step was to send the interview questions to the security coordinator, the employees from other departments of the public organization in Morocco.

The second part of this document deals with the development of an information systems security policy in a large organization (for confidentiality reasons, we will not be able to disclose the organization's name). The objective of this policy will be to provide a coherent, recognized and shared security framework between all the organization's stakeholders, to enable the implementation and ensure the long-term security of their information systems and to define a coordinated action plan enabling each entity to better address its own challenges.

The case study took place at a large organization in Morocco. The extended time required for the study was a result of difficult access to the subjects as well as multiple visits to subjects. The security officer was interviewed four times and the CIO was interviewed three times. During the course of the

study, both the CIO and security officer have removed from their positions and new employees replaced them. This required yet more follow up interviews.

The objective is to draw up a macroscopic inventory of the level of security of all information systems, assets and people at the organizational and technological levels. For this purpose, we have developed a questionnaire whose analysis of the responses recorded in it will make it possible to evaluate the levels of maturity of the IS. In this context, we refer, for this exhaustive questionnaire, to the standard ISO/IEC 27002:2013 as defined in the Appendix (Table 4).

The study found that the organization has an information security policy and helps the organization successfully manage information security. The organization security maturity is at the level 2(initial). The organization agrees that the Information Security Policy is an important tool that organizations should have in order to manage the proper implementation of information security.

The information security policy is deployed during an awareness session and is explained to senior management and the heads of each section. Following the session, each section head is responsible for communicating and disseminating all information regarding the information security policy to end users within each section.

The organization uses a type of information security policy, which helps to protect information in general.

The organization information security policy document is understandable, which means that employees can understand the content of the policy. One interviewee explained that “Our organization’s information security policy is written to be understood by all in order to follow the meaning of the policy. It is also placed on a very easy to access place on the net, internal (intranet) and external (website).

The person responsible for creating the information security policy is the security manager with the support of the IT department. The municipality uses ISO 27001 and ISO 27002 as a guide in its work. The organization places a high priority on information security policy, starting with senior management and reaching end users.

The information security policy is the main document that was intended for the organization. Organizations should have a structure and procedures on which policies should exist and how they are developed, and the organization should take this into account. What do you call politics? For example, operational policy (which probably includes elements other than information security), security policy (which addresses security issues) or information

security policy is the responsibility of each organization. The important thing is that management must show its intentions regarding information security.

The policy should not contain concrete rules of conduct without expressing management's intentions and thus frame the other documents that govern it. A policy should be brief and accessible to all. More information and explanations can be presented on the internal web for example. The policy expresses the general intentions of management. When it comes to information security policy, it can be called information security policy or security policy if it applies to all security work. The policy should be developed at an early stage, before or at the same time as activities determine security design and security processes. It is important to identify all existing policy documents to know what material you need to work with. This gives an idea of the work required to prepare regulatory documents and to put policy documents in order. The working group can then update and draft policy documents in the order that corresponds to the organization's information security needs.

The scheme of declination of the PSSI is shown in Figure 6.

ISSP Global Plan

The Information Systems Security Policy is generally composed of two parts:

- The Security Policy Framework
- Security principles and rules

Preamble

For confidentiality reasons, we are not authorized to disclose the corporate name of the organization. For this reason, we use the name SECT_PUBLIC

Figure 6. The scheme of declination of the PSSI

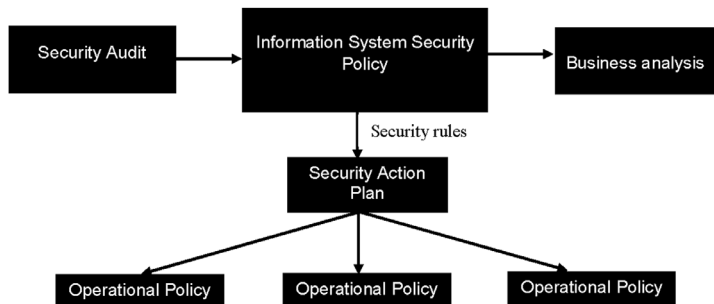
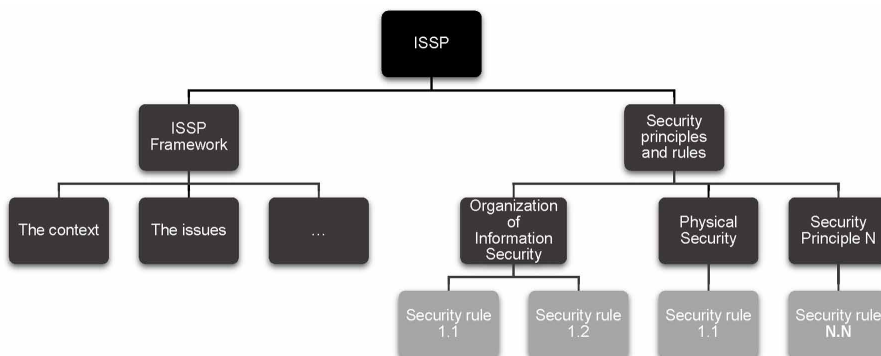


Figure 7. ISSP global plan



to indicate the name of the organization. This document constitutes the reference, also called “Information Systems Security Policy” (ISSP) of the SECT_PUBLIC. It is based on the ISO 27002 standard (good practice guide for information security). It translates into applicable terms the will and requirements of the SECT_PUBLIC to implement the means to protect in the most effective way the heritage represented by Information Systems, with all its resources (information and their various means of sharing, processing, exchange and storage), and to preserve its operation as a production tool for users.

Context

The SECT_PUBLIC has a patrimony of sensitive information constituting one of its most important assets, on which its image and its capacity to maintain and develop its activities are based:

- The information heritage, composed of all the information contributing to its knowledge and know-how
- Information contributing to the functioning of the Union such as financial data
- Information relating to personnel, such as administrative files, pay slips, etc.
- Information relating to its user-customers and third parties with whom it has a relationship.

Perimeter

The ISSP applies to all the Information Systems (IS) of the SECT_PUBLIC. This includes all the human, technical and organizational means enabling, in support of the activity, to create, store, exchange and share information between the internal and external actors of the organization, whatever the form in which it is used (electronic, printed, handwritten, voice, images, etc.). It applies:

- To all personnel authorized to access, use or process information or information system resources of the SECT_PUBLIC
- On a contractual basis, to all third parties, as soon as they use the IS of SECT_PUBLIC or their own IS is connected to the IT network of SECT_PUBLIC
- All hardware and software components of the Information System.

ISSP Issues in the Sect_Public

Information Systems Security (ISS) is an essential component of the protection of the PUBLIC_SECT in its own interests and in those related to the issues related to its activity. This requires, as a priority, the definition and implementation within the PUBLIC_SECT of an “Information Systems Security Policy” (ISSP) to manage the:

- Risk of unavailability of information and the systems processing it (intrusion, theft, destruction, breakdown, denial of service)
- Risk of disclosure - loss of accidental or voluntary confidentiality of sensitive information such as personal data, remote management data, strategic documents, financial data, etc.
- Risk of alteration - loss of integrity, particularly in the context of institutional site data, video protection, etc.

Its objectives are:

- Define the target in terms of Information Systems Security management,
- Organise security
- Comply with the regulations in force
- Federating around the theme of security
- Monitor and improve safety on a daily basis.

- The security rules set out in the PSSI are supplemented by operational policies (rules for the use of the information system, internal rules, password policy, backup, etc.).

Security Requirements

The Information Systems Security needs of the SECT_PUBLIC are based on four criteria (AICD):

- **Availability:** Guarantee that the elements considered (files, messages, applications, services) are accessible at the desired time by the authorized persons
- **Integrity:** Ensure that the elements considered (data, messages...) are accurate and complete and that they have not been modified
- **Confidentiality:** Guarantee that only authorized persons to have access to the elements considered (applications, files...)
- **Data Recovery Point:** Ensure that data is restored following a loss according to its criticality.

SECURITY CLAUSES

Organization of Information Security

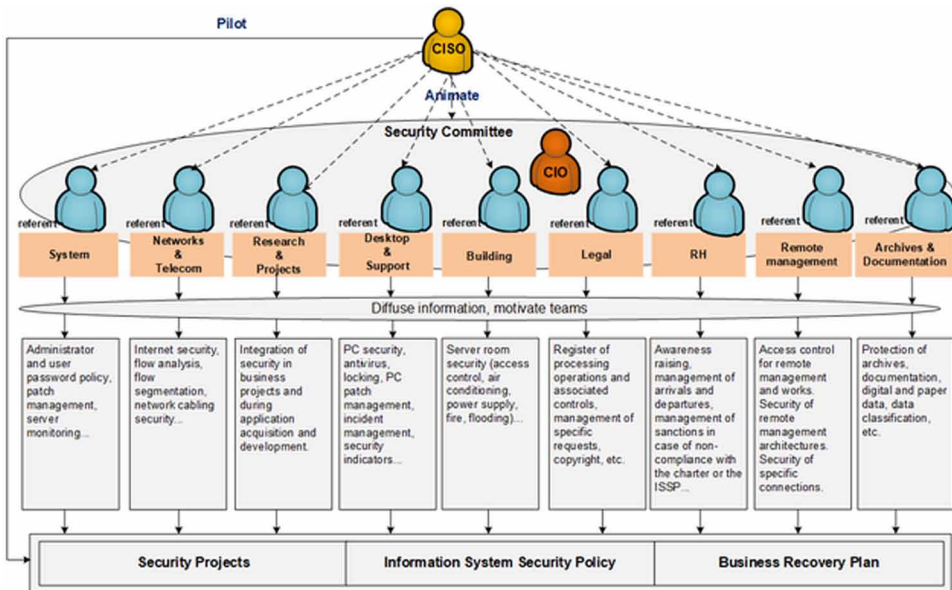
Internal Organization

In order to manage, monitor and guarantee the security of information within the SECT_PUBLIC in a transversal way, the following organization is implemented as shown in Figure 8.

The Information Security Committee (ISC), composed of the Information System Security Officer (ISSO), the Information System Officer (CIO), the security referents and guests as appropriate (agent, third parties, etc.), has the following objectives:

- Guarantee the same level of information to the different referents
- To provide feedback and exchange on each other's good practices in the field of information security
- Define operational policies

Figure 8. Organization of security diagram



- Prioritize and distribute the different projects among the referents
- Propose and arbitrate the training plan for the referents
- Coordinate safety awareness and communication actions
- Organise safety/compliance audits
- Report on security incidents
- Integrate and share technical, legal and regulatory intelligence
- Manage exceptions (event not taken into account in the PSSI) having an impact on the security of the Information Systems of the SECT_PUBLIC.

The Information Systems Security Officer (ISSO) has a coordinating role in the implementation and application of the PSSI of the SECT_PUBLIC. It does not intervene directly at the operational level as prime contractor for security projects, but:

- Leads the ISC
- Manages the Information Systems Security Policy and controls its application
- Coordinates the day-to-day management of the security function
- Ensures the management of transversal safety projects

Information Security Policy in Large Public Organizations

- Participates in the homogenization of the security level
- Ensures the perenniality of Security
- Defines, implements, analyses and monitors major security indicators in coordination with the ISC
- Keeps abreast of the state of the art in the field of Information Systems.

The security referents are responsible for security watch (legal, regulatory, technical) according to their scope of intervention.

Third Party Management

When SECT_PUBLIC entrusts third parties with the management and control of all or part of its Information Systems (outsourcing, outsourcing, etc.), it integrates its security requirements into the contracts with them.

Information System Security Policy

The information security policy constitutes the reference framework for information security within Sec_Public. It therefore defines the various rules to be observed and the work methodology to be implemented in order to understand the security issues of the information system.

Objectives

Sec_Public's information system security policy aims to ensure:

- Compliance with any legislation or regulatory obligation in Morocco and with any internal Bank policy and regulations, in particular laws 07-03, 53-05 and 09-08 governing information security at the national level;
- The protection of the information assets essential to the performance of its activities,
- Minimize the risk of information unavailability or alteration
- Ensure and guarantee the brand image.

Scope of the IS Security Policy

The IS Security Policy applies to the following assets:

- Computer, network and telecom equipment
- Software and computer data
- Information system services
- Bank premises at central and regional level
- Human Resources

Review and Evaluation

The security policy must be reviewed regularly. Regular reassessment (at least once a year) ensures its relevance and effectiveness. The organization of this revision is the responsibility of the Sec_Public ISSR.

Compliance With Policy

Sec_Public requires any natural or legal person who accesses its information to respect the information security policy as well as the procedures, charters and measures that result from it.

Asset Management

Property Inventory

An inventory of all assets (activities, data, applications and infrastructures) of the information system must be carried out. This inventory should not be limited to physical assets. Inventory monitoring and updating must also be ensured. An owner must be designated for each asset (activities, data, applications and infrastructure). The IS security officer must be responsible for updating the inventory.

Classification of Information and Assets

Assets (activities, data, applications and infrastructures) must be classified in terms of values, legal or regulatory requirements, sensitivity or criticality with respect to availability, integrity, confidentiality and traceability (DICT) criteria.

Such classification makes it possible to better fight against threats that could harm Sec_Public. The impact analysis conducted by the process owner,

assisted by the safety manager, enables the value of the IS asset and therefore its sensitivity level to be assessed.

Human Resources Security

Transfer and Departure of Staff

Any transfer or departure of an employee automatically entails the updating or the suppression of all his access rights. The new access rights are decided by the line manager according to the employee's new tasks. The departments and services concerned must notify the Information System Department, by a note, of any change in the status of an employee.

Information Security Awareness and Training

The IS Security Policy must be assimilated, implemented and maintained at all levels of the organization. The involvement of all employees is necessary for this policy to be a success and for the defined level of safety to be achieved.

Users must be made aware of information security issues, threats and good practices. They must thus be able to support Sec_Public's security policy within the normal and daily framework of their work.

Physical and Environmental Safety

Access to Buildings

SEC_PUBLIC has taken measures to restrict access to its buildings. All visitors and external speakers must identify themselves and wear a badge in a visible manner throughout their visit on the Sec_Public site.

Security Service

A security service (from 7 am to 7 pm) ensures the physical security and operation of the Sec_Public building. The security service is provided by an external company.

In this sense, the security service must record the CIN number of visitors in the access register.

A remote monitoring system must be put in place.

Datacenter Security

Security zones must be located and protected to reduce the risks posed by environmental threats and hazards (fire, flood, earthquake, explosion, or other types of natural disasters). The following measures may be required to enhance physical security:

- Automatic fire detection and suppression systems
- Protection against water damage
- Air conditioning safety
- Protection against electrical incidents
- Surveillance cameras
- False floors
- Protection against physical access

Disposal of Such Sensitive Assets

Equipment used to store sensitive information (data) for disposal must be destroyed effectively to prevent any attempt at recovery.

Operations Management

Development of Operating Procedures

Operational procedures related to the management and operation of information processing facilities shall be documented and maintained. The management and use of information processing resources must be formalized through operational procedures. These procedures shall include the measures necessary to address the security needs expressed.

Backup Procedures

A backup policy must be defined for sensitive or critical Sec_Public information, applications and systems based on the analysis of business impacts carried out in collaboration with information owners and business departments.

Backups must be performed regularly, tested and protected appropriately. Regular recovery tests ensure that backups have been performed correctly

and that backup media is readable. To ensure the protection of backup media, the following steps can be taken:

- Conservation at a remote site,
- Storage in a secure location (fireproof box, locked cabinet).

Management of Traceability of Operations

Traceability of safety-related operations and events must be ensured. Traces of these events must also be kept secure. Regular analyses and reviews of trace files should be performed by the CISO.

Use of Communication Tools (Internet, Intranet, Messaging)

Information technologies, such as the Internet or e-mail, are necessary tools for business activities. However, their advantageous features may present risks related to the Sec_Public environment.

The use of communication tools must be regulated and integrated into Sec_Public's information resources use charter.

Particular attention should be paid to the presence of wireless networks that could compromise the access control devices envisaged.

Maintenance of Assets if and Environmental Equipment

IT assets (servers, databases, network, workstations, etc.) and environmental equipment (inverters, fire detection systems, etc.) must be properly maintained to ensure their proper operation.

This maintenance must be carried out on a regular basis to avoid incidents related to equipment obsolescence and poor maintenance.

External IT Service Providers

Suppliers, external consultants and subcontractors working for Sec_Public are subject to Sec_Public's information security policy. External providers who access the information system must sign a confidentiality agreement that defines the roles, rights and obligations that the provider must comply with to guarantee.

Access Controls

System Access Control Standard

All users of the IT system must have an identifier to ensure optimal management of access controls, individual accountability and the creation of complete audit reports. The user ID linked to a user must not be shared. Shared identifiers must be limited and restricted in use.

Workstation and Equipment

It is a question of controlling allocations for strictly professional needs through:

- The deactivation of the administrator account;
- Internet filtering;
- Disabling USB Flash Drives;
- Standardization of positions.

Password Management

Users should follow good security practices when selecting and using passwords. In accordance with the password policy defined within Sec_Public, rules must be defined to ensure proper password management.

Network Partitioning

The implementation of control measures within the network to isolate groups of information services, users and information systems should be considered.

Cryptography

Cryptographic Controls

Confidential information within SEC_Public must be encrypted using valid encryption processes for data at rest and in motion, as required by state or federal laws or regulations. This includes but is not limited to sensitive information stored on mobile devices, removable disks and laptops.

Cryptographic Authentication

Public Sec Information system must obtain and issue public key and Transport Layer Security (TLS) certificates from an approved service provider. This control focuses certificates with visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services. Secure Socket Layer (SSL) protocol must be disabled on all devices.

System Acquisition, Development and Maintenance of Information Security

Separation of Development and Production Facilities

As far as possible, development, test and production environments should be separated according to the risks involved. The transfer of programmes and information must be controlled. The development and testing environment must be independent and separate from the production environment. The production environment must be installed on machines that will not be used simultaneously in development or test environments. A developer must not access production.

Integrating Security Into Projects Development

Sec_Public's statements of requirements for the acquisition of new systems or for improvements to existing systems shall specify the requirements for security measures.

SUPPLIER RELATIONSHIPS

Information Security Incident Management

A procedure to ensure the recording and reporting of any security incident must be defined. Users (Bank staff, contractors and third-party users with access to the information system) must be informed of their obligation to report any security incident (loss/theft of Sec_Public information, documents or material) as soon as possible.

Sec_Public's incident management procedure includes reporting mechanisms for these incidents and a specific organization for handling security alerts.

Information Security Aspects of Business Continuity Management

Business continuity and business resumption plans must be developed to maintain or restore Sec_Public's critical activities within the required timeframe after an interruption or failure of their critical processes.

The continuity plan integrates preventive and curative measures enabling a business management to overcome a major incident by reducing the impact on its activities to an acceptable level.

These continuity plans must indicate the conditions under which they are triggered, the organization of the implementation, the crisis management measures, the detailed planning of the actions to be carried out, the communication plans, the means used for crisis management,...

A disaster scenario approach is preferred in order to consider the various scenarios (e.g. fire, destruction of the computer room, unavailability of premises, etc.) and to plan appropriate corrective measures (e.g. regular extraction of vital information on paper, redundancy of sensitive environments).

The emergency site in Tangier must meet international standards in terms of physical security.

Compliance

Identification and Communication of Applicable Legislation

All legal, regulatory and contractual requirements must be identified and documented for each information system. These regulatory requirements may include the following:

- Protection of personal data,
- Respect for intellectual property (for example: keeping proof of software purchase, maximum number of users allowed on a system, information to staff on legal issues).

IS Security Audit

Information security should be audited and monitored periodically. The audit should focus on compliance with security policies and procedures and on the effectiveness of the security measures put in place and their adequacy to the potential risks identified.

Access to security audit tools and reports must be protected to prevent possible misuse or compromise.

CONCLUSION

The objective of this study was to establish a practical framework for the formulation and implementation of the IS security policy. The problem arising from this situation is an ineffective IS security policy and therefore a vulnerable system. To achieve this objective, we reviewed the ISO 20002 security policy frameworks and put in place

During this part, the document called Information System Security Policy (ISSP) was set up, which reflects Sec_Public will and requirements to implement the means to protect in the most effective way the heritage represented by Information Systems, with all its resources (information and their various means of sharing, processing, exchange and storage), and to preserve its operation as a production tool for users.

Further research is needed to determine situation within more controlled environments, such as commercial or private organizations. Being a state educational entity may have distorted the results to a degree and having additional, more diverse data would validate the framework to a greater level. Also, this study focused on the relatively small subset of those most directly involved in policy. A quantitative examination of a wide base of users might shed some additional light on policy implementation.

REFERENCES

Ahmad, A., & Ruighaver, A. (2003). Improved event logging for security and forensics: Developing audit management infrastructure requirements. *Proceedings of the ISOneWorld*.

- Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, 15(5/6), 337–346. doi:10.1108/09576050210447019
- Burns, E. (2010). Developing Email Interview Practices in Qualitative Research. *Sociological Research Online*, 15(4), 1–12. doi:10.5153ro.2232
- Calder, A., & Watkins, S. G. (2010). *Information security risk management for ISO27001/ISO27002*. It Governata.
- Canavan, S. (2003). *An information security policy development guide for large companies*. SANS Institute.
- Coyne, J. W., & Kluksdahl, N. C. (1994). Automated Information Systems Security Engineering (a Case Study in Security Run Amok). In *Proceedings of the 2Nd ACM Conference on Computer and Communications Security* (pp. 251–257). New York: ACM. 10.1145/191177.191241
- Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.
- Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, 61, 169–183. doi:10.1016/j.cose.2016.06.002
- Fomin, V. V. (2008). Iso/Iec 27001 Information Systems Security Management Standard : Exploring the Reasons for Low Adoption, (February 2016), 1–13.
- Gikas, C. (2010). A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. *Information Security Journal: A Global Perspective*, 19(3), 132–141. doi:10.1080/19393551003657019
- Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal*, 23(4), 367–376. doi:10.1108/17542731111139455
- Glasgow, J., Macewen, G., & Panangaden, P. (1992). A Logic for Reasoning About Security. *ACM Transactions on Computer Systems*, 10(3), 226–264. doi:10.1145/146937.146940
- Höne, K., & Eloff, J. H. (2002a). What Makes an Effective Information Security Policy? *Network Security*, 2002(6), 14–16. doi:10.1016/S1353-4858(02)06011-7

- Höne, K., & Eloff, J. H. P. (2002b). Information security policy — what do international information security standards say? *Computers & Security*, *21*(5), 402–409. doi:10.1016/S0167-4048(02)00504-7
- Hong, K., Chi, Y., Chao, L. R., & Tang, J. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, *14*(2), 104–115. doi:10.1108/09685220610655861
- Howcroft, T. (2005). *Handbook of Critical Information Systems Research*. Northampton: Edward Elgar Publishing, Inc.
- Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79. doi:10.1016/j.im.2013.10.001
- ISECT. (2012). *ISO 27001 Security*. Retrieved September 2012, from ISO 27001 Security: http://www.iso27001security.com/html_27002.html#HistoryOfISO17799
- ISO/IEC. (2005). ISO 27002: 2005. Information Technology-Security Techniques-Code of Practice for Information Security Management.
- ISO/IEC. (2013). *ISO/IEC 27002:2013*. Retrieved March 24, 2014 from Http://www.iso.org/iso/home/store_catalogue_ics/catalogue_detail_ics.htm?csnumber=54533
- Johnson, B. G. (2014). *Measuring ISO 27001 ISMS processes*. Academic Press.
- Joshi, J., Ghafoor, A., Aref, W. G., & Spafford, E. H. (2001). Digital government security infrastructure design challenges. *Computer*, *34*(2), 66–72. doi:10.1109/2.901169
- Knapp, K., Morris, R., E. Marshall, T., & Byrd, T. (2009). Information security policy: An organizational-level process model. *Computers & Security* (Vol. 28). doi:10.1016/j.cose.2009.07.001
- Knapp, K. J., Marshall, T. E., Rainer, R. K. Jr, & Ford, F. N. (2007). Information Security Effectiveness: Conceptualization and Validation of a Theory. *International Journal of Information Security and Privacy*, *1*(2), 88–112. doi:10.4018/jisp.2007040103
- Kühnhauser, W. E. (1999). Policy Groups. *Computers & Security*, *18*(4), 351–363. doi:10.1016/S0167-4048(99)80081-9

- Maleh, Y. (2018). *Security and Privacy Management, Techniques, and Protocols*. Hershey, PA: IGI Global; doi:10.4018/978-1-5225-5583-4
- Mintzberg, H. (1983). *Structures in Fives: Designing Effective Organizations*. Englewood Cliffs, NJ: Prentice Hall.
- Mintzberg, H., Lampel, J., & Quinn, J. B. (2003). *The Strategy Process. Concepts. Context. Cases (4th ed.)*. Upper Saddle River, NJ: Pearson Education, Prentice Hall.
- Peltier, T. R. (2013). *Information Security Fundamentals (2nd ed.)*. Taylor & Francis. doi:10.1201/b15573
- Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC Press.
- PRGL. (2011). Retrieved March 4, 2012, from Praxiom Research Group Limited: <http://www.praxiom.com/iso-17799-intro.htm>
- Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIREs: A Policy Framework for Information Security. *Communications of the ACM*, 46(7), 101–106. doi:10.1145/792704.792706
- Reich, B. H., & Benbasat, I. (2000). Factors That Influence the Social Dimension of Alignment between Business and Information Technology Objectives. *Management Information Systems Quarterly*, 24(1), 81–113. doi:10.2307/3250980
- Talib, M. A., El Barachi, M., Khelifi, A., & Ormandjieva, O. (2012). Guide to ISO 27001: UAE case study. *Issues in Informing Science and Information Technology*, 7, 331–349.
- Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, 24(2), 99–104. doi:10.1016/j.cose.2005.02.002
- Walsham, G. (1993). *Interpreting information systems in organizations*. John Wiley & Sons, Inc.
- Willison, R. A. (2002). *Opportunities for computer abuse: Assessing a crime specific approach in the case of Barings Bank*. PhD Thesis.
- Yassine, M., & Abdelkebir, S., & Abdellah, E. (2017). A Capability Maturity Framework for IT Security Governance in Organizations. *13th International Symposium on Information Assurance and Security (IAS 17)*.

KEY TERMS AND DEFINITIONS

Access Control: Ensures that resources are only granted to those users who are entitled to them.

Asset: Anything that has a value to the organizations.

Audit: Information gathering and analysis of assets, processes, and controls to ensure policy compliance.

Authentication: The process of verifying a claim of identity. Three different types of information can be used for authentication: something you know (a PIN, a password, mother's maiden name), something you have (magnetic swipe card) or something you are (biometrics).

Availability: Information and supporting IT systems should be available to authorized users when needed.

Confidentiality: Data or information prevented from the exposure to unauthorized individuals is labeled as confidential.

Encryption: The action of changing the information by using an algorithm to make it unreadable to anyone.

Incident Management: An Area of the IT service management that help to restore service operation to normal as fast as can be done after an incident has occurred, and reduce the negative impact on business operations.

Information Security Policy: A written, living document outlining the actions and procedures that employees should follow in order to protect an organization's information security assets, an information security policy outlines the function and tasks of employees in order to protect an organization's information assets.

Integrity: Integrity is the quality of being whole, uncorrupted and complete.

ISMS: An information security management system (ISMS) is a tool that helps organizations to establish, implement, operate, monitor, review, maintain and improve the desired level of information security in the organization.

ISO/IEC 27001:2013: Information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information Technology – Security Techniques – Information Security Management Systems – Requirements.

ISO/IEC 27002:2013: Information security standard (list of controls) published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information Technology – Security Techniques – Code of practice for Information Security – Controls.

Risk Assessment: The analysis of the possible hazards that could occur within a workplace and finding a solution to reduce the risk. This is avoiding injury to an individuals and damage to property.

Third Party: Person or body that is recognized as being independent of the organization.

Top Management: High level management.

Vulnerability: A weakness in the organization, network that can be exploited by a threat.

APPENDIX

Table 4. ISO 27002 domains and questions

Domain	No.	ISO Section Question	Process Self Assessment Rating (From 0 to 5)
Information security policies		Management direction for information security	
	1	Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy? (as specified in ISO/IEC 27001 section 5.2.)	
	2	Periodic review of policies and feedback (eg, every 12 months?)	
	3	Thoroughness and completeness of policies and standards (see comments)	
Organization of information security		Internal organization	
	4	Is there an information security function responsible for security initiatives within the organization?	
	5	Contacts with relevant external authorities (such as CERTs and special interest groups) on information security matters.	
	6	Do external parties have access to Scoped Systems and Data or processing facilities? If so, rate the maturity of the controls around reviewing third party contracts, active controls and monitoring/auditing	
Organization of information security		Mobile Devices and Teleworking	
	7	Policy/Standard and guidelines specific for mobile devices (laptops, mobile phones, tablets, etc)	
	8	Policy/Standard and guidelines for remote work locations, and remote virtual conferencing	
Human resource security		Prior to employment	
	9	Are security roles and responsibilities of constituents defined and documented in accordance with the organization's information security policy?	
	10	Is a background screening performed prior to allowing constituent access to Scoped Systems and Data?	
	11	Are new hires required to sign any agreements upon hire?	
Human resource security		During employment	
	12	Is there a disciplinary process for non-compliance with information security policies? (employees and contractors)	
	13	Security Awareness Training Program;	

continued on following page

Table 4. Continued

Human resource security		Termination and change of employment	
	14	Is there a constituent termination or change of status process? A person's exit from the organization or significant changes of roles should be managed; returning corporate information and equipment, updating access rights.	
Asset management		Responsibility for assets	
	15	Is there an asset management policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy? (see comment)	
	16	Information assets should be inventoried and owners should be identified to be held accountable for their security.	
	17	Is there insurance coverage for business interruptions or general services interruption?	
Asset management		Information classification	
	18	Information should be classified and labelled by its owners according to the security protection needed, and handled appropriately.(see comment)	
Asset management		Media handling	
	19	Asset decommissioning, reuse, disposal and physical media security. Information storage media should be managed, controlled, moved and disposed of in such a way that the information content is not compromised.	
Access control		Business requirements of access control	
	20	The organization's requirements to control access to information assets should be clearly documented in an access control policy and procedures.	
	21	Electronic systems; adherence to principle of least privilege, separation of duties, role based access controls	
	22	Multi factor authentication for critical services	
	23	Isolation of environments and assets within those environments (e.g., Production, Development, Staging)	
	24	Remote Access Access Controls and Auditing	
Access control		User access management	
	25	Processes and Procedures regarding account creation, modification and revocation.	
	26	Special restrictions for privileged access rights and the management of passwords	
	27	Review and audit of access controls, accounts and entitlements	
Access control		User responsibilities	
	28	Internal Security Training (aside from security awareness)	

continued on following page

Information Security Policy in Large Public Organizations

Table 4. Continued

Access control		System and application access control	
	29	Information access should be restricted in accordance with the access control policy e.g. through secure log-on, password management, control over privileged utilities and restricted access to program source code.	
Cryptography		Cryptographic Controls	
	30	Are there standards in place to dictate cryptographic best practices? (the use of encryption, cryptographic authentication and integrity controls such as digital signatures and message authentication codes, key management)	
	31	Utilization of cryptographic controls following best practices, providing confidentiality and integrity with respect to scope systems and data	
Physical and environmental security		Secure areas	
	32	Is there a physical security program for scoped systems and environments where scoped data is stored and processed?	
	33	Are reasonable physical security and environmental controls present in the building/data center that contains Scoped Systems and Data? Have these controls been audited and/or certified by an independent third party?	
Physical and environmental security		Equipment Security	
	34	Equipment should not be taken off-site unless authorized, and must be adequately protected both on and off-site.	
	35	Information must be destroyed prior to storage media being disposed of or re-used. Unattended equipment must be secured	
Operations management		Operational procedures and responsibilities	
	36	IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Capacity and performance should be managed. Development, test and operational systems should be separated.	
Operations management		Protection from malware	
	37	For all scoped systems and networks, malware controls are required, including user awareness.	
Operations management		Backup	
	38	Appropriate backups should be taken and retained in accordance with a backup policy.	

continued on following page

Table 4. Continued

Operations management		Logging and monitoring	
	39	For all scoped systems and systems containing scoped data, system user and administrator/operator activities, exceptions, faults and information security events should be logged and protected. Clocks should be synchronized.	
Operations management		Control of operational software	
	40	Software installation on scoped operational systems should be controlled.	
Operations management		Technical vulnerability management	
	41	For scoped systems, vulnerabilities should be actively identified and patched.	
Operations management		Information systems audit considerations	
	42	IT audits should be planned and controlled to minimize adverse effects on production systems, or inappropriate data access.	
Communications security		Network security management	
	43	Networks and network services should be secured and hardened.	
Communications security		Information transfer	
	44	There should be policies, procedures and agreements (e.g. non-disclosure agreements and security control clauses) concerning information transfer to/from third parties, including electronic messaging.	
System acquisition, development and maintenance		Security requirements of information systems	
	45	Security control requirements should be analyzed and specified, including web applications and transactions.	
	46	Are systems and applications patched?	
	47	Are vulnerability tests (internal/external) performed on all applications at least annually?	
System acquisition, development and maintenance		Security in development and support processes	
	48	Rules governing secure software/systems development should be defined as policy. Changes to systems (both applications and operating systems) should be controlled.	

continued on following page

Information Security Policy in Large Public Organizations

Table 4. Continued

	49	Software packages should ideally not be modified, and secure system engineering principles should be followed. The development environment should be secured, and outsourced development should be controlled.	
	50	System security should be tested and acceptance criteria defined to include security aspects.	
System acquisition, development and maintenance		Test data	
	51	Test data should be carefully selected/generated and controlled.	
Supplier relationships		Information security in supplier relationships	
	52	There should be policies, procedures, awareness etc. to protect the organization's information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed within the contracts or agreements.	
Supplier relationships		Supplier service delivery management	
	53	Service delivery by external suppliers should be monitored, and reviewed/audited against the contracts/agreements. Service changes should be controlled.	
Information security incident management		Management of information security incidents and improvements	
	54	Responsibilities and procedures exist to manage (report, assess, respond to and learn from) information security events, incidents and weaknesses consistently and effectively, and to collect forensic evidence.	
Information security aspects of business continuity management		Information security continuity	
	55	The continuity of information security should be planned, implemented and reviewed as an integral part of the organization's business continuity management systems.	
Information security aspects of business continuity management		Redundancies	
	56	Is there a documented policy for business continuity and disaster recovery that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	
	57	Is there an annual schedule of required tests and testing occurs?	
	58	Is a Business Impact Analysis conducted at least annually? (to confirm SLA commitments)	

continued on following page

Table 4. Continued

Compliance		Compliance with legal and contractual requirements	
	59	The organization must identify and document its obligations to external authorities and other third parties in relation to information security, including intellectual property, records, privacy/personally identifiable information and cryptography.	
Compliance		Information security reviews	
	60	There an internal audit, risk management or compliance department with responsibility for identifying and tracking resolution of outstanding regulatory issues	
	61	The organization's information security arrangements are independently reviewed (audited) and reported to management.	
	62	Managers routinely review employees' and systems' compliance with security policies, procedures etc. and initiate corrective actions where necessary.	

Conclusion

This chapter presents a summarized review of the book. The Strategic Information Technology Governance Frameworks and Models are described in Chapters 1 and 2. This includes material on different Information Technology Governance definitions, issues and frameworks. Chapter 3 provides a practical framework to evaluate Information Technology in Large Organizations. This chapter includes a review of related theories along with an applied discussion of IT Governance aspects including use, strategy, and an adoption by large organizations. The Chapters 4-6 investigate Information Technology Agility in Large Organizations. Those include IT agility survey, Maturity Framework for IT agility, and cloud computing for managing IT Agility are described in separate chapters. The last three chapters describe Information Security Governance in Large Organizations by exploring the engagement processes and the practices of organizations involved in a strategy of information security governance in Chapter 7. A Capability Maturity Framework for information security governance in a large organization in Chapter 8. Finally, the Chapter 9 aims to guide organizations in their approach to implementing an effective Information Security Policy through ISO 27002.

REVIEW OF CHAPTERS

Introduction

This chapter provided the background for the book; introduced the research including the problem being addressed, the motivation for the research and the book contributions.

Chapter 1: From Information Governance to IT Governance – An Overview of Issues and Frameworks for Large Organizations

This chapter represented an opportunity to reflect on the issues related to information in organizations and to examine closely, without claiming to be exhaustive, the difficulties and challenges they face; the value of information in companies and the interest of organizing it. The main objective of this chapter is to provide a state of the art on information governance and IT governance definitions, issues and frameworks.

Chapter 2: A Deep Overview of Information Technology Governance Standards

This chapter presented the state of the art of research on the practice of information technology (IT) governance through an analysis of the various proposed standards. This analysis was conducted based on a meta-model of 4 worlds. This chapter is organized as follows: in the first part, we describe the proposed reference framework for the IS governance domain. Five recognized approaches are then evaluated under this framework.

Chapter 3: Evaluation of IT Governance in Middle East and North African Large Organizations

The chapter explored how best-practice frameworks, such as the COBIT model, can be adapted to conduct evaluations of IT governance within medium and large organizations and to further explore the factors that influence the acceptance and adoption of the adapted framework. Four sub-research questions were answered and a research model proposed and supported in order to address the primary objective of the research.

The research findings reinforce the important role of frameworks in IT governance evaluation. Employing an approach based on innovation adoption theory enables the understanding of the factors related to acceptance of IT governance frameworks, providing practitioners with additional knowledge and thus enabling a better understanding, and hence influencing, the adoption of IT governance frameworks.

Chapter 4: Strategic Agility Frameworks for Information System Governance

This chapter presented different frameworks and models have been presented and studied, with the aim of proposing a specific model that encompasses the advantages of different approaches. The objective of this research is to contribute to the understanding of strategic agility of the information system (IS). The chapter summarized all existing knowledge in an agility framework that encompasses the advantages of different approaches. Scientists and practitioners can exploit this framework to develop criteria and measures to assess the strategic agility of the IS. This is an important improvement since agility is a fundamental characteristic of an information system in terms of strategic value.

Chapter 5: IT Management Agility in Large Organizations – A Case Study

This chapter presented a global, practical and agile framework for supporting IT Service management ITSM. The proposed framework surpasses the limitations of existing methods/referential and meets the needs of international standards regarding flexibility and agility to improve ITSM processes. An efficient, agile and practical approach to ITSM is vital for IT organizations to increase the quality of services they provide, to improve speed and agility of the service desk, and to improve user experience, all reducing the cost to run IT. The chapter aims to identify the important aspects that propose a practical agile framework for ITSM efficiency. It was collected based on a theoretical and empirical research study that generated answers to the sub-level research questions, and a return of experience analysis of the best practices in organizations.

This generic framework will help any organization in the implementation of an agile, secure and optimal IT Service Center. The proposed framework is measured by adopting a continuous improvement process based on DevOps (DevOps is the concatenation of the first three letters of the word “development” and the usual abbreviation “ops” of the word “operations”) and the PDCA Deming cycle.

Chapter 6: Managing the Cloud for Information Technology Agility in Large Organizations

This chapter identified the determinants of cloud-computing adoption based on innovation characteristics and the technology, organization, and environmental contexts of organizations, and evaluate how cloud computing changes IS agility, it started. A research model was developed that integrates the DOI theory and the TOE framework. The model was empirically evaluated based on a semi-structured interview with IT experts. It was used to compare the adoption of cloud computing in two distinct sectors, namely manufacturing and services. The results indicated that Agility, relative advantage, complexity, technological readiness, top management support, and firm size have a direct effect on a firm's adoption of cloud computing. The analysis of results validated the direct effect of Agility on cloud-computing adoption. In addition, we compiled four groups of attributes into a framework proposed for consideration in the consideration of IS agility, A survey was built based on Agility attributes. The data were collected from employees of 10 on a sample of 10 different large companies in Europe (France, UK, Spain, Switzerland, and Germany). Drawing on research findings, we concluded that some cloud computing service models improve specific dimensions of agility, for example, IaaS increases technical infrastructure agility. PaaS improves human characteristics while SaaS does not associate with any category.

Chapter 7: Information Security Governance Practices and Commitments in Organizations

This chapter explored the determinants of organizations' involvement in the information security governance and their practices in this area. The survey conducted among two hundred large organizations proposes a model consisting of seven determinants of the commitment of organizations in the information security governance process: it suggested that the knowledge of organizations engaged in the governance of security Information or promotion, the performance expected and the effort deployed to encourage the commitment of organizations in the process. The responses to the questionnaire also increase awareness of current practices of information security governance implemented by organizations.

By this empirical study and the results of our survey, a framework for measuring the maturity of information security was proposed with the aim of providing a practical tool for measuring and improving governance

Conclusion

of information security in the organization. To show the effectiveness of the proposed framework, the authors implemented the resultant maturity framework in a large organization. The results will be presented in Chapter 8.

Chapter 8: Information Security Governance in Large Organizations – A Maturity Framework

This chapter proposed a framework for measuring the maturity of information security was proposed with the aim of providing a practical tool for measuring and improving governance of information security in the organization based on best practices from organizations as described in Chapter 7. The proposed information security governance framework has been implemented in a medium organization to drive and improve the maturity of information security governance. The results are satisfactory and prove that the model will be able to provide great support to organizations in different sizes and various sectors of activity in their governance and management of information security. Nevertheless, it is suggested that the scientific community and organizations adopt this framework and test it in different case studies.

This research has shown how organizations implement information security governance. A grounded case study strategy answered the research question and developed practice using the procedures and techniques of grounded practice methodology discussed in the previous chapter of this book.

While existing research has focused on the implementation of information security governance and it is recognized that it is not possible to have a completely secure environment, research has found that the close relationship between risk management, information security governance, and compliance is critical to achieving objectives.

Chapter 9: Information Security Policy in Large Public Organizations – A Case Study Through ISO 27002

This chapter guided organizations in their approach to implementing an IT Security policy. The purpose of the first part of this chapter was to discover how information security controls are selected. To achieve this objective, information security managers from six large MENA organizations were interviewed. The second part of this chapter presented a practical model of IT security policy based on ISO/IEC 27002:2013 through a case study in a large public organization.

There are very few scientific papers on ISO 27002, and none found that research practice uses ISO 27002 controls as described in the background section. This chapter can be considered exploratory: The data collected in this research may well be used to formulate hypotheses for other research projects.

CONCLUSION

This chapter has presented a review of the book. It has been suggested in this book to address the issue of strategic IT governance in large organizations through three critical areas, maturity of IT governance in large organizations, IT agility, and information systems security. This book explores the characteristics of IT governance in large organizations in order to give readers (students, IT professionals, and researchers) a theoretical and practical basis for understanding IT governance, and to provide decision-makers the necessary tools to succeed their IT governance strategy in the organization.

About the Authors

Yassine Maleh is from Morocco. He is a PhD of the University Hassan 1st in Morocco in the field of Internet of Things Security and privacy, since 2013. He is IT Senior Analyst at the National Port Agency in Morocco. He is Member of IEEE Communications Society and European Microwave Association, the International Association of Engineers IAENG and The Machine Intelligence Research Labs. Maleh has made contributions in the fields of information security and Privacy, Internet of Things Security, Wireless and Constrained Networks Security. His research interests include Information Security and Privacy, Internet of Things, Networks Security, Information system and IT Governance. He has published over than 50 papers (Book chapters, international journals and conferences/workshops), and 2 edited books “Security and Privacy in Smart Sensor Networks” and “Security and Privacy Management, Techniques, and Protocols”. He serves as an Associate Editor for the International Journal of Digital Crime and Forensics (IJDCF) and the International Journal of Information Security and Privacy (IJISP). He was also a Guest Editor of a special issue on Recent Advances on Cyber Security and Privacy for Cloud-of-Things of the International Journal of Digital Crime and Forensics (IJDCF), Volume 10, Issue 3, July-September 2019. He has served and continues to serve on the executive and technical program committees and a reviewer of more than 150 papers for numerous international conference and journals such as Ad hoc Networks, IEEE Sensor Journal, ICT Express, International Journal of Computers and Applications, IEEE Transactions on Network Science and Engineering, Journal of Cases on Information Technology (JCIT), International Journal of Cyber Warfare and Terrorism (IJCWT). He received Publons Top 1% reviewer of the year 2018 award.

Sahid Abdelkbir is from Morocco. He is a PhD Student at the National School of Business and Management (ENCG) in Settati, Morocco, since 2014. He received his Master degree (2012) in Computer Sciences from the Faculty of Science and Technology Settati, Morocco, and his Bachelor in Networks and IT Systems (2009) from Hassan 1st University Morocco. He is the author and co-author of more than 14 papers including journals, conferences, chapters, and books, which appeared in refereed specialized journals and symposia. His research interests include Information Systems, IT Agility, IT Service Management and IT Security.

Mustapha Belaissaoui is a Professor of Computer Science at Hassan 1st University, Settati, Morocco, he is a deputy director of the National School of Business and Management (ENCG) Settati, and Head of Master Management Information System and Communication in the same Business School. He obtained his PhD in Artificial Intelligence from Mohammed V University in Rabat. His research interests are Combinatorial Optimization, Artificial Intelligence and Information Systems. He is the author and co-author of more than 70 papers including journals, conferences, chapters, and books, which appeared in refereed specialized journals and symposia.

Index

A

Access Control 365, 387-388, 395
 Agility 129, 138-140, 142-149, 151, 153-155, 158-162, 172-174, 176, 179-180, 182-183, 185, 198, 200, 203, 205, 207, 214, 216, 230-236, 240, 243, 249-250, 253, 256, 258-259, 261-265
 Asset 2, 47, 59, 75, 123, 172, 174, 176, 179, 185, 188-189, 191-192, 195, 207, 214, 225, 294-295, 301, 365, 375, 384-385, 395
 Audit 33, 48, 55, 67-68, 96, 98, 107, 209-210, 213, 237, 296, 301, 322, 329, 356, 360, 366, 388, 391, 395
 Authentication 366, 374, 389, 395
 Availability 138, 186, 188-189, 197, 234, 246, 255, 303, 323-324, 351, 366, 368, 384, 395

B

best approaches 138
 best practices 5, 33, 48, 66, 70-71, 92-93, 95-96, 106, 174, 176, 182, 185, 282, 302-303, 318, 322

C

Capability 63, 68, 70, 73-74, 94, 99-101, 107, 117-123, 127-128, 144, 151-152, 182, 233, 282, 306, 316, 318, 324, 327, 332

Case study 33, 83, 92, 95, 97, 105, 112, 114, 118, 120, 129, 172, 178-179, 184, 286-287, 321, 340-341, 349, 356, 371, 376
 Cloud Computing 216, 230-240, 243-247, 249-250, 253-256, 258, 260-262, 264-265, 277
 CMMI 59, 63, 66, 70-71, 73-74, 77, 80, 82
 COBIT (Control Objectives for Information and Related Technologies) 1, 3, 18-20, 33, 47, 49-50, 59, 65-71, 80, 82, 92-94, 96-101, 103-108, 111-112, 117-119, 122-123, 127-129, 176, 178-179, 318, 322, 330, 352
 COBIT 5 1, 33, 69, 96, 100-101, 107-108, 111, 118-119, 122-123, 128
 commitments 280, 282, 292, 302-303, 316
 competitive advantages 138
 Confidentiality 157, 254, 303, 323, 351, 364-367, 369, 376, 378, 384, 387, 395
 COSO 65-66, 75-76, 80, 82

D

Data Collection 105-108, 118-119, 207, 225, 250, 258, 288, 329, 361
 Definitions 1, 3-4, 6, 18-19, 33, 96, 140, 142, 161
 DevOps 172, 176, 182-183, 200, 205-207, 213-214, 230
 Diffusion of Innovations Theory (DOI) 277
 digital technologies, 2

E

Encryption 254, 388, 395

G

Governance 1-6, 8-12, 17-20, 29-31, 33, 47-55, 57, 59-70, 80-83, 92-99, 101-108, 111-112, 114, 117-120, 123, 125, 127-129, 138, 142, 150, 172, 176, 193, 205, 210, 234, 265, 280-288, 290-304, 306, 308-309, 316-319, 321-324, 326, 329, 333, 339-341

H

health sector 4

Higher Education 31, 96-97

I

IaaS (Infrastructure as a Service) 231, 235, 262-265, 277

Incident 186-188, 200, 204, 209, 211-212, 215, 225, 244, 283, 351, 360-361, 368, 376, 389-390, 395

Incident Management 186-188, 200, 204, 211-212, 215, 225, 283, 368, 389-390, 395

Information governance 1-6, 10-12, 17, 50, 107-108, 286, 320

information security 14, 51, 77-78, 80, 82, 98-99, 182, 197, 210, 265, 280-288, 290-303, 306-307, 309, 316-324, 326-327, 329, 333, 340-341, 349-355, 357-364, 367-369, 372-379, 381, 383-385, 387, 389-391, 395

Information Security Policy 284-285, 299, 320-321, 349-350, 353-354, 372-375, 377-378, 383-384, 387, 395

Information System 47, 57, 63, 66-67, 92-93, 118, 138-139, 148-149, 156, 162, 188, 230, 233-234, 281, 292, 301, 340, 351-352, 356, 381, 383-385, 387, 389-391

Information Systems 4, 19, 30, 47, 54, 64, 67, 80, 92, 96-97, 102, 104-105, 109, 138-140, 142-143, 150, 152, 160, 162, 176, 179, 230, 233, 239, 249-250, 256, 258, 265, 287, 303, 321, 323, 349, 351, 358, 361, 363, 366-367, 376-383, 388, 391

Integrity 254, 303, 323, 351, 365-366, 384, 395

ISMS 77, 352-353, 358-359, 369-370, 395

IT Asset Management 59, 176, 179, 189, 195, 207, 225

IT governance 1, 3-4, 6-7, 9-10, 17-20, 29, 31, 33, 47-53, 55, 57, 59-62, 64-70, 80-83, 92-99, 101-107, 111-112, 114, 117-120, 125, 127-129, 172, 205, 282, 285-286, 298, 301, 320, 322-323

IT Processes 30, 53, 55-57, 61, 67-69, 71, 96-101, 105, 107-108, 110-112, 117-118, 120-123, 125, 127, 173-174, 178-179, 198, 203-204

IT Security 196-198, 207, 210, 213, 282, 291, 294-296, 302, 317-318, 372

IT Service Management 66, 129, 162, 173-179, 184-185, 188, 207, 211-213, 215, 225, 395

ITAM 176-177, 180, 182-185, 189, 191-193, 195-196, 198, 200, 203, 205-209, 215, 225

ITIL 18, 49-50, 65-66, 70-73, 80, 82, 95, 174, 176-179, 185, 189, 205, 209

ITSM 172-178, 180, 182-185, 189, 196, 198, 200, 203, 205-212, 214-216, 225

L

Large organizations 1, 17, 33, 83, 92, 94, 102-103, 105-106, 108, 127, 129, 172, 249, 256, 259, 265, 309, 316, 370

M

Maturity 18, 47, 50, 59, 62-63, 66-68, 70, 73-74, 94-95, 97-99, 107, 118, 120-123, 128, 162, 172-173, 177, 179, 183, 189, 192, 197-198, 205-211, 213-214,

Index

- 225, 233, 282, 284, 286-287, 296-298, 302-304, 306, 309, 316, 318, 320-321, 323-324, 326-327, 329-333, 339-340, 349, 358, 371, 373-374, 377
- Maturity Model 63, 70, 73, 99, 189, 192, 205-206, 214, 225, 286, 320, 358, 371
- mixed approach 102-103
- ## **O**
- Organization strategy 138
- ## **P**
- PaaS (Platform as a Service) 235, 263-265, 278
- Performance Measurement 47, 67, 74, 96
- PMBOOK 77
- policy 9, 11, 15, 17, 138, 148, 160, 196-197, 284-285, 294, 299, 320-321, 349-357, 359, 363, 365, 368, 372-376, 378-380, 383-388, 391, 395
- practices 2, 5, 7, 13, 15, 19, 33, 47-48, 66-67, 70-71, 77, 80-81, 83, 92-93, 95-96, 98, 106-107, 118, 120, 138, 150, 162, 174, 176-177, 179-180, 182, 184-185, 200, 205, 209, 215, 244-245, 265, 280-282, 285-286, 291, 295-296, 302-304, 309, 316-320, 322-324, 331, 333, 339, 353, 358, 361, 363, 385, 388
- ## **R**
- Resource Management 19, 47, 176, 284
- Risk Assessment 75, 339, 362, 372, 396
- Risk Management 1, 3-4, 7, 11, 19, 33, 47, 58, 65, 75, 295-296, 301, 318-319, 341, 351
- ## **S**
- SaaS (Software as a Service) 188, 235, 263-265, 278, 375
- Standards 5, 7-8, 19, 33, 48-50, 64, 66-67, 71, 77, 80, 82, 93-95, 160, 175-176, 179, 183, 216, 244, 247, 254, 256, 280, 282, 292, 307, 316, 318, 323, 327, 351, 357-358, 360, 362, 369, 390
- Strategic Alignment 1, 3, 7, 17, 19, 47, 58, 65, 93, 182, 294
- ## **T**
- technical evolutions 138
- technological solutions 317
- Technology Organization Environment (TOE) 278
- Third Party 375, 383, 396
- Top Management 107, 160, 243, 246, 255, 265, 293, 299, 355, 396
- ## **U**
- Use-Case 225
- ## **V**
- Value Delivery 19, 30, 47, 65
- Vulnerability 160, 281, 295-296, 317, 366, 396