

Management for Professionals



Steven De Haes
Wim Van Grembergen

Enterprise Governance of Information Technology

Achieving Alignment and Value,
Featuring COBIT 5

Second Edition

 Springer

Management for Professionals

More information about this series at <http://www.springer.com/series/10101>

Steven De Haes • Wim Van Grembergen

Enterprise Governance of Information Technology

Achieving Alignment and Value,
Featuring COBIT 5

Second Edition



Springer

Steven De Haes
Information Technology Alignment
and Governance Research Institute
University of Antwerp - Antwerp
Management School
Antwerp, Belgium

Wim Van Grembergen
Information Technology Alignment
and Governance Research Institute
University of Antwerp - Antwerp
Management School
Antwerp, Belgium

ISSN 2192-8096
Management for Professionals
ISBN 978-3-319-14546-4
DOI 10.1007/978-3-319-14547-1

ISSN 2192-810X (electronic)
ISBN 978-3-319-14547-1 (eBook)

Library of Congress Control Number: 2015932080

Springer Cham Heidelberg New York Dordrecht London
© Springer Science+Business Media, LLC 2009
© Springer International Publishing Switzerland 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media
(www.springer.com)

Preface

“Enterprise Governance of IT” is a relatively new concept in the literature and is gaining more and more interest in the academic and practitioner’s world. “Enterprise Governance of IT” is about defining and embedding processes and structures in the organization that enable both business and IT people to execute their responsibilities in creating value from IT-enabled business investments. As an example of its growing importance, the standardization organization ISO issued in 2008 a new worldwide ISO standard in this domain.

Within the University of Antwerp–Antwerp Management School–IT Alignment and Governance (ITAG) Research Institute, we have been executing applied research in this domain for many years now. With this book, we want to provide a complete and comprehensive overview of what Enterprise Governance of IT entails and how it can be applied in practice. Our conclusions in this book are based on our knowledge obtained in applied research projects, our many years of involvement in the development of COBIT, our own hands-on coaching and consulting experience in many industries in governance and alignment projects, and international state-of-the-art literature. In this way, this manuscript encompasses both academic models and concepts but also includes practice-oriented frameworks such as COBIT and discusses and analyzes many practical cases and examples in different industries.

The target audience for this book is threefold:

- Master students, for whom this textbook can be used in courses typical on IT strategy, Enterprise Governance of IT, IT management, IT processes, IT and business architecture, IT assurance/audit, information systems management, etc.
- Executive students in business schools, for MBA type of courses where IT strategy or IT management modules are addressed.
- Practitioners in the field, both business and IT managers, who are seeking research-based fundamentals and practical implementation issues related to it in the domain of Enterprise Governance of IT.

This book is organized into seven main chapters. Chapter 1 defines the core concepts around Enterprise Governance of IT as a means to enable business/IT

alignment and business value from IT. This chapter sets the scene of the complete book. Chapter 2 builds on the first chapter and stipulates a conceptual model to address the challenge of implementing Enterprise Governance of IT in practice. This chapter also provides an overview of contemporary best practices organizations are using and addresses related topics on, for example, the role of the board of directors in Enterprise Governance of IT and the context of interorganizational environments. In Chap. 3, the impact of Enterprise Governance of IT implementations on business/IT alignment is discussed. The first question is how an organization can measure and evaluate its current status of business/IT alignment. This discussion is supplemented with a benchmarking case, where business/IT alignment was measured for the Belgian financial services sector. Next, the impact of Enterprise Governance of IT practices on business/IT alignment is analyzed and illustrated. Chapter 4 discusses the value component of this textbook. It starts from describing the IT productivity paradox and then discusses two approaches to measure and manage the value of IT, at the level of an investment through the business case process and at the level of the IT department through the IT balanced scorecard. Chapter 4 also includes a detailed case study of a working IT balanced scorecard implementation. Chapter 5 positions COBIT in the field of Enterprise Governance of IT. This chapter discusses in detail all the core elements of the COBIT framework and explains how organizations could leverage them for the purpose of Enterprise Governance of IT. Related to this, Chap. 6 continues by discussing how COBIT can also be leveraged as a framework to execute IT assurance/audit assignments. This chapter also offers a lot of hands-on templates that can be used in practice. Chapter 7 finally provides some guidelines and trigger events to get started with Enterprise Governance of IT and outlines a balanced scorecard for Enterprise Governance of IT to manage and measure the outcome of the enterprise governance of IT project.

To support the reader in understanding and absorbing the material provided, each chapter provides (short and long) “assignment boxes” where readers can apply the concepts explained in comprehensive exercises. Also, at the end of each chapter, a summary and study questions are available enabling the reader to cross-check the insights obtained in a chapter. For people who want more information, each chapter provides hooks to more detailed background material by way of literature references.

We hope that with this book, we can contribute to further developing the emerging knowledge domain of Enterprise Governance of IT. This book is one of the outcomes of our activities within the University of Antwerp–Antwerp Management School–IT Alignment and Governance (ITAG) Research Institute. We do welcome reactions on this book or sharing experiences in the domain of Enterprise Governance of IT via steven.dehaes@uantwerpen.be and wim.vangrembergen@uantwerpen.be.

Antwerp, Belgium
January 2015

Steven De Haes
Wim Van Grembergen

Acknowledgments

We would like to thank all participants involved in our research and teaching activities and in writing this book. Without the support of these people, the development of this book could not have been satisfactorily completed.

We gratefully acknowledge the business and IT managers who shared their insights and practices on Enterprise Governance of IT and participated in one or more of our research projects. We appreciate support provided for this project by the Business Faculty of the University of Antwerp and the Antwerp Management School, by our colleagues in these institutions, and by other international colleagues we had the opportunity and honor to work with. We also would like to thank our master and executive students who provided us with many ideas on the subject of Enterprise Governance of IT and its related mechanisms.

We would also like to express our gratitude toward the board of directors, the management committee, and all the staff and volunteers of the ISACA. Our involvement in the COBIT development activities has been of great value in further progressing our ideas.

We also thank Springer who showed great interest in our research and book project and from whom we received magnificent support in managing this project.

Finally, last but not least, we would like to thank our families. Wim would like to extend his gratitude to Hilde, Astrid, and Helen who always supported and helped him with every project including this book. Steven wishes to thank Brenda for her loving support and patience and wants to dedicate this book to Ruben, Charlotte, and Michiel.

Contents

1 Enterprise Governance of IT, Alignment and Value.....	1
1.1 Enterprise Governance of IT in the Context of Digitized Organizations	1
1.2 Business/IT Alignment	4
1.3 Value from IT	6
Summary	8
Study Questions	9
References.....	9
2 Enterprise Governance of IT	11
2.1 Practices for Implementing Enterprise Governance of IT	11
2.2 Principles for Enterprise Governance of IT	18
2.3 Case Study: Enterprise Governance of IT at KLM.....	19
2.3.1 KLM's Trigger Points to Start the Journey	20
2.3.2 Embarking on the Journey	21
2.3.3 Reported Benefits.....	29
2.4 Enterprise Governance of IT and the Board	32
2.5 Intraorganizational Governance of IT	36
2.6 Theoretical View on EGIT: Viable Systems Theory.....	37
2.6.1 System 1: The Productive Function	39
2.6.2 System 2: The Coordination Function	39
2.6.3 System 3: The Executive Function	40
2.6.4 System 4: The Planning and Future Focus Function	40
2.6.5 System 5: The Coherence Function	40
2.7 Applying the VSM in the Context of Enterprise Governance of IT	40
Summary	42
Study Questions	42
References.....	43

3 Business/IT Alignment.....	45
3.1 Measuring Business/IT Alignment	45
3.1.1 The Matching and Moderation Approach.....	45
3.1.2 The Profile Deviation Approach	47
3.1.3 The Scoring Approach	47
3.1.4 The Maturity Model Approach	50
3.2 Aligning Business Goals and IT Goals.....	50
3.3 The Relationship Between Enterprise Governance of IT and Alignment.....	54
3.4 Exploring Culture and Alignment.....	56
3.4.1 The Hofstede Framework for Studying National Culture.....	57
3.4.2 Applying the Hofstede Framework to Explore the Impact of Culture on Business and IT Alignment	58
3.4.3 Conceptually Comparing Alignment Cultural Differences Between Belgium and the Netherlands	62
3.4.4 Empirically Comparing Alignment Cultural Differences Between Belgium and the Netherlands	65
Summary	69
Study Questions	69
References.....	69
4 IT-Enabled Value.....	71
4.1 The IT Black Hole	71
4.2 The Business Case Process	72
4.3 The Balanced Scorecard	79
4.3.1 IT BSC Core Concepts.....	79
4.3.2 Mini-Case.....	83
4.3.3 Corporate Contribution Perspective	88
4.3.4 Customer Orientation Perspective	91
4.3.5 Operational Excellence Perspective.....	93
4.3.6 Future Orientation Perspective.....	94
Summary	99
Study Questions	99
References.....	100
5 COBIT as a Framework for Enterprise Governance of IT	103
5.1 COBIT History.....	103
5.2 COBIT 5 Principles.....	104
5.2.1 Meeting Stakeholder Needs: Strategic Business/IT Alignment	104
5.2.2 Meeting Stakeholder Needs: The Balanced Scorecard	106
5.2.3 Covering the Enterprise End-to-End: IT Savviness	106
5.2.4 Applying a Single, Integrated Framework: COBIT/RISKIT/VALIT	110
5.2.5 Applying a Single Integrated Framework: IT Savviness	112

5.2.6	Enabling a Holistic Approach: Organizational Systems.....	113
5.2.7	Separating Governance from Management: ISO/IEC 38500.....	114
5.3	COBIT 5 Enabling Processes and Domains	115
5.3.1	Process Description and Purpose	115
5.3.2	Goals and Metrics	115
5.3.3	RACI Chart	117
5.3.4	Management Practices and Inputs/Outputs.....	118
5.3.5	Management Practices and Activities	119
5.4	Translating COBIT to Your Practice.....	120
5.4.1	Scoping COBIT	120
5.4.2	Turning COBIT Process into Practice: Example EDM2—Benefits Delivery	120
5.4.3	Turning COBIT Process into Practice: Example APO5—Portfolio Management	122
5.5	COBIT Process Maturity and Process Capability.....	123
5.6	COBIT 5 Product Family	125
5.7	COBIT 5 Benchmarking	126
	Summary	126
	Study Questions	127
	References.....	128
6	COBIT as a Framework for IT Assurance	129
6.1	IT Assurance and COBIT 5	129
6.2	Building an IT Assurance Function	131
6.2.1	Structures for IT Assurance	131
6.2.2	Processes for IT Assurance	132
6.2.3	Principles, Policies, and Frameworks for IT Assurance	134
6.2.4	Culture, Ethics, and Behavior for IT Assurance	135
6.2.5	Information for IT Assurance	135
6.2.6	Services, Infrastructure, and Applications for IT Assurance	138
6.2.7	People, Skills, and Competencies for IT Assurance	139
6.3	Executing the IT Assurance Process.....	139
6.3.1	Determining the Scope of the Assurance Assignment.....	140
6.3.2	Executing the IT Assurance Initiative.....	141
6.3.3	Communicate and Report	142
6.4	IT Assurance in Practice	144
6.4.1	Templates for Scoping	144
6.4.2	Templates for Testing.....	146
	Summary	148
	Study Questions	149
	References.....	149

7 Guidelines for the Implementation of Enterprise	
Governance of IT	151
7.1 Key Success Factors in the Case of KLM.....	151
7.2 Getting Started: Pain Points and Trigger Events.....	153
7.3 Measuring and Managing the Process of Enterprise Governance of IT	154
7.3.1 Building an Enterprise Governance of IT BSC	154
7.3.2 Metrics for an Enterprise Governance of IT BSC.....	155
Summary	162
Study Questions	163
References.....	163
Index.....	165

About the Authors

Steven De Haes is an associate professor of Information Systems Management at the University of Antwerp and Antwerp Management School. He is actively engaged in teaching and applied research in the domains of digital strategies, IT governance and management, IT strategy and alignment, IT value and performance management, IT assurance and audit, and information risk and security.

He teaches at bachelor, master, and executive level and acts as Academic Director for the Executive Master of IT Governance and Assurance, the Executive Master of Enterprise IT Architecture, and the Master in Management. His research has been published in international peer-reviewed journals and conference proceedings, and he has coauthored and/or edited several books. He is coeditor-in-chief of the *International Journal on IT/Business Alignment and Governance* (www.igi-global.com/ijitbag) and acts as Academic Director of the IT Alignment and Governance (ITAG) Research Institute.

He recently held positions of Director of Research and Associate Dean Master Programs for the Antwerp Management School. He also acts as speaker and facilitator in academic and professional conferences and coaches organizations in their digital strategies, IT governance, and alignment and assurance efforts. He is involved in the development of the international IT governance framework COBIT as researcher and coauthor.

He can be contacted at steven.dehaes@uantwerpen.be.

Wim Van Grembergen is a professor at the Economics and Management Faculty of the University of Antwerp (UA), past-chair of the MIS department (UA), and executive professor at the Antwerp Management School (AMS). He was previously a guest professor at the University of Leuven (KUL) and had teaching assignments at the University of Stellenbosch in South Africa, the Institute of Business Studies in Moscow, the Queensland University of Technology in Australia, Simon Fraser University in Canada, and the University of Cape Town in South Africa. From 1989 to 1995, he served as Academic Director of the MBA Program of UFSIA (now UA). He is past academic director of the Executive Master of IT Governance and Assurance and the Executive Master of Enterprise IT Architecture (AMS).

Over the last 14 years, he conducted research in IT governance, IT audit, IT strategy, IT performance management, and the IT balanced scorecard.

Dr. Van Grembergen presented at leading conferences such as the European Conference on Information Systems (ECIS), the Information Resources Management Association (IRMA) Conference, and the Hawaii International Conference on Systems Sciences (HICSS). Since 2002, he is mini-track chair “IT governance and his mechanisms” at the HICSS conference. He has many publications in leading academic journals and published books on IT governance and the IT balanced scorecard. He is coeditor-in-chief of the *International Journal on IT/Business Alignment and Governance*. As founder of the IT Alignment and Governance (ITAG) Research Institute, he is involved in research for ISACA/ITGI on IT governance and supports the continuous development of COBIT. He was involved in the development of the recently published COBIT 5 framework. Dr. Van Grembergen is a frequent speaker at academic and professional meetings and conferences and has served in a consulting capacity to a number of firms. His e-mail address is wim.vangrembergen@uantwerpen.be

Chapter 1

Enterprise Governance of IT, Alignment and Value

Abstract The main title of this book refers to the concept of Enterprise Governance of IT, a concept that addresses the definition and implementation of processes, structures, and relational mechanism that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of value from IT-enabled business investments. The subtitle of the book also introduces two other important concepts, namely business/IT alignment and IT-enabled value. In this introductory chapter, these three core constructs are defined and connected to each other and placed in the context of the digitized organization. Each of these concepts will then be further developed in the following chapters.

1.1 Enterprise Governance of IT in the Context of Digitized Organizations

Information technology (IT) has become crucial in the support, sustainability, and growth of enterprises. Previously, governing boards and senior management executives could delegate, ignore, or avoid IT decisions. In most sectors and industries, such attitudes are now impossible, as enterprises are increasingly completely dependent on IT for survival and growth.

In commerce marked by increasingly global horizontal and vertically integrated value chains, system and network downtime has become far too costly for most enterprises. These organizations also face a wide spectrum of external threats, including abuse, cybercrime, fraud, errors, and omissions. At the same time, IT has the potential to support both existing business strategies, but also to shape new strategies. Or in the words of Hirt and Wilmmott in their McKinsey report on strategic principles for competing in the digital age: “Digital capabilities increasingly will determine which companies create or lose value” (Hirt and Wilmmott 2014). In this viewpoint, IT moves from commodity service provider to strategic partner within the digitized enterprise (De Haes and Van Grembergen 2009; Weill and Ross 2004).

Given the centrality of IT for enterprise risk management and value generation, a specific focus on enterprise governance of IT (EGIT) has arisen over the last two decades (De Haes and Van Grembergen 2009; Thorp 2003; Wilkin and Chenhall 2010).

Enterprise governance of IT (EGIT) is an integral part of corporate governance, exercised by the Board, overseeing the definition and implementation of processes, structures and relational mechanism in the organisation 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 business investments.

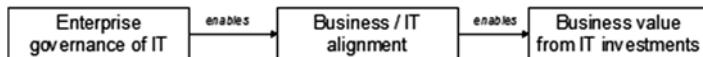


Fig. 1.1 Definition of enterprise governance of IT

Assignment Box 1.1: “IT Doesn’t Matter”

Not everybody seems to agree with the increasing strategic importance of information technology. In his article “IT doesn’t matter,” Nicolas Carr ([2003](#)) makes the comparison between commodities such as water and gas, and information technology. He states, “As information technology’s power and ubiquity have grown, its strategic importance has diminished. [...] By now, the core functions of IT—data storage, data processing, and data transport—have become available to all. Their very power and presence have begun to transform them from potentially strategic resources into commodity factors of production. They are becoming costs of doing business that must be paid by all but provide distinction to none.”

Look up the article of Nicolas Carr and the discussions on the Internet that resulted after his article. Summarize your thoughts and present a critical view to your peers.

In the context of this book, EGIT is defined as stated in Fig. 1.1. The definition not only refers to EGIT as an organizational capacity (e.g., structures and processes), but also to the outcomes it enables, specifically business/IT alignment and in the end more value creation out of IT-enabled investments. The conceptual model as visually presented in Fig. 1.1 has also been validated by other researchers, including Wu et al. ([forthcoming](#), p. 1) who conclude in their research: “we uncover a positive, significant, and impactful linkage between IT governance mechanisms and strategic alignment and, further, between strategic alignment and organizational performance.”

It is not clear when exactly the concept of “Enterprise Governance of IT,” as we understand it now, originated. Gartner introduced the idea of “Improving IT governance” for the first time in their Top-ten CIO Management Priorities for 2003 (ranked third). In 1998, the IT Governance Institute (www.itgi.org) was founded to disperse the IT governance concept. In academic and professional literature, articles mentioning IT governance in the title began to emerge late 1990s. In the context of the leading academic conference, Hawaii International Conference on Systems Sciences (HICSS) IT governance was defined as organizational capacity exercised by the board, executive management, and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT (Van Grembergen 2002).

After the emergence of the IT governance concepts, the notion received a lot of attention. However, due to the focus on “IT” in the naming of the concept, the IT governance discussion mainly stayed a discussion within the IT area. We have experienced this in our research many times, where we tried to contact the CEO for an interview on IT governance issues and immediately got transferred to the CIO. In the field, many IT governance implementations are driven by IT, while one would expect that the business would and should take a leading role here as well. It is clear that business value from IT investments cannot be realized by IT, but will always be created at the business side. For example, there will be no business value created when IT delivers a new CRM (Customer Relationship Management) application on time, on budget and within functionalities, and when afterwards the business is not integrating the new IT system into its business operations. Business value will only be created when new and adequate business processes are designed and executed enabling the sales people of the organization to increase turnover and profit (De Haes and Van Grembergen 2009; Thorp 2003).

This discussion raised the issue that the involvement of business is crucial and initiated a shift in the definition, focusing on the business involvement, towards “enterprise governance of IT.” As defined in previous section, EGIT is an integral part of corporate governance exercised by the board overseeing 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.

EGIT clearly goes beyond the IT-related responsibilities and expands towards (IT-related) business processes needed for business value creation. Also the standardization organization ISO moved into this direction, with the release in 2008 a new worldwide standard defined as “Corporate Governance of IT” (ISO/IEC 38500 2008). In this standard, ISO puts forward six principles for governance of IT, addressing both business’ and IT’s roles and responsibilities, that express preferred behavior to guide IT-related decision making. In the same line of thinking, ISACA complemented its IT governance best practices framework COBIT 4 (ISACA 2007), focusing on IT processes and responsibilities, with the Val IT framework and

RISKIT framework (ISACA 2008, 2009), addressing the business processes and responsibilities in value creation and risk management. We have been, and still are, involved in the development of these frameworks and have experienced this broadening view towards EGIT as very enriching evolution within the ISACA frameworks. The broadened view of end-to-end responsibilities in IT governance is now fully embedded in the COBIT 5 framework that was issued in 2012 (ISACA 2012; De Haes et al. 2013). More information about this COBIT 5 framework is discussed in Chap. 5.

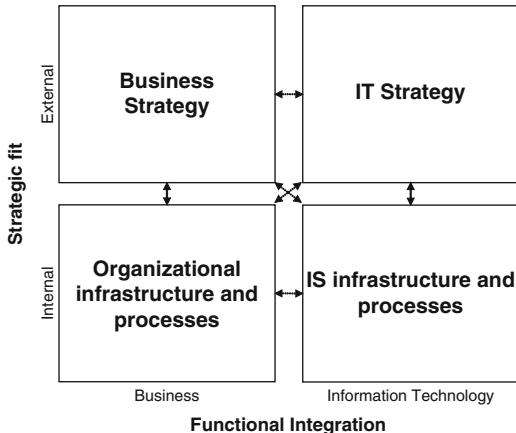
This change in naming and focus from “IT Governance” to “Enterprise Governance of IT” might appear subtle and not groundbreaking, but it implies a crucial shift in the minds of business people. The leading role of IT people in IT governance has always been a paradox. The same thing happened in the era of business process reengineering, where also in many cases IT took a leading role reinventing business processes. It is however clear that business processes and business value creation can and should only be in the ownership of business people. On the other hand, we have to acknowledge that in practice, this mind shift will not happen by itself or by changing the name of the concepts. We believe that the CIO office in general and the CIO in specific is often in a unique position to act as a change agent in the organization and to realize the business buy-in over time. The latter will also be illustrated in the KLM case study as discussed in the next chapter of this book.

1.2 Business/IT Alignment

The EGIT definition explicitly underlines that the outcome of EGIT is the alignment of information technology with the business. This section will provide some initial insights into the business/IT alignment concept. Note that business/IT alignment is discussed in more detail in Chap. 3, including the relationship between EGIT and business/IT alignment.

What does “alignment between the business and IT” exactly mean? Business/IT alignment is the fit and integration among business strategy, IT strategy, business structures, and IT structures. It comprises two major questions: how is IT aligned with the business and how is the business aligned with IT. Henderson and Venkatraman (1993) were the first to clearly describe the interrelationship between business and IT in their well-known Strategic Alignment Model or SAM model (see Fig. 1.2). Many authors used this model for further research. The concept of the SAM model is based on two building blocks: “strategic fit” and “functional integration.” *Strategic fit* recognizes that the IT strategy should be articulated in terms of an external domain (how the firm is positioned in the IT marketplace) and an internal domain (how the IT infrastructure should be configured and managed). Strategic fit is of course equally relevant in the business domain. Two types of *functional integration* exist: strategic and operational integration. Strategic integration is the link between business strategy and IT strategy reflecting the external components which are important for many companies as IT emerged as a source of strategic advantage.

Fig. 1.2 Strategic alignment model. Adapted from: Henderson, J.C. and Venkatraman, N., 1993, Strategic alignment: leveraging Information Technology for transforming organizations, IBM Systems Journal, vol. 32, no. 1

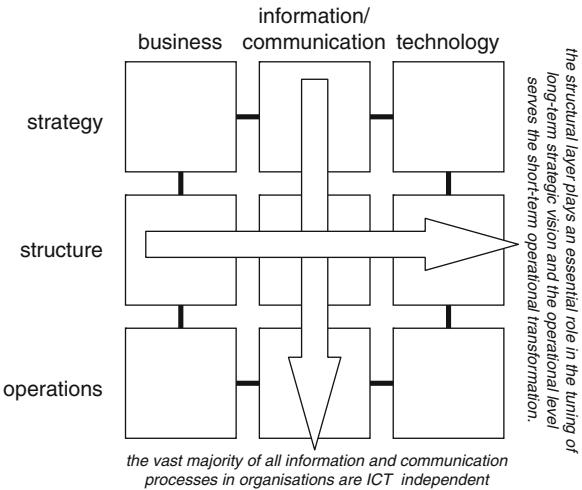


Operational integration covers the internal domain and deals with the link between organizational infrastructure and processes and IT infrastructure and processes.

Henderson and Venkatraman argue that the external and the internal domain are equally important, but that managers traditionally think of IT strategy in terms of the internal domain, since historically IT was viewed as a support function that was less essential to the business. In their research results, Henderson and Venkatraman warn of the problems that may surface when a bivariate approach is undertaken with respect to balancing across the four domains—IT strategy, business strategy, IS infrastructure, and organizational infrastructure—is used. For instance, when only external issues—IT strategy and business strategy—are considered, a serious underestimation of the importance of internal issues such as the required redesigning of key business processes might occur. Therefore, SAM calls for the recognition of multivariate relationships, which will always take into consideration at least three out of the four defined domains.

The SAM model demonstrates that alignment is a multi-faced and complex construct, often referred to as the alignment challenge. Broadbent and Weill (1998) continue in this domain by depicting a number of difficulties (barriers) that organizations have experienced while aligning business with IT. The *expression barriers* arise from the organization's strategic context and from senior management behavior, including lack of direction in business strategy. This results in insufficient understanding of and commitment to the organization's strategic focus by operational management. *Specification barriers* arise from the circumstances of the organization's IT strategy such as lack of IT involvement in strategy development and business and IT management conducting two independent monologues. This ends up in a situation where business and IT strategies are set in isolation and are not adequately related. The nature of the organization's current IT portfolio creates *implementation barriers* which arise when there are technical, political, or financial constraints on the current infrastructure. A good example of this last barrier is the difficult integration of legacy systems.

Fig. 1.3 The alignment framework of Maes—an extension of SAM. Adapted from: Maes R., 1999, Reconsidering Information Management through a Generic Framework, PrimaVera Working Paper 99-15



Many authors have used the SAM model for further research and have provided comments and additional insights. Maes (1999) for example developed an interesting extension to the Strategic Alignment Model (see Fig. 1.3). The basic idea is that the 2×2 dimensions of the Strategic Alignment Model is an oversimplification of reality and needs to be extended to a 3×3 model.

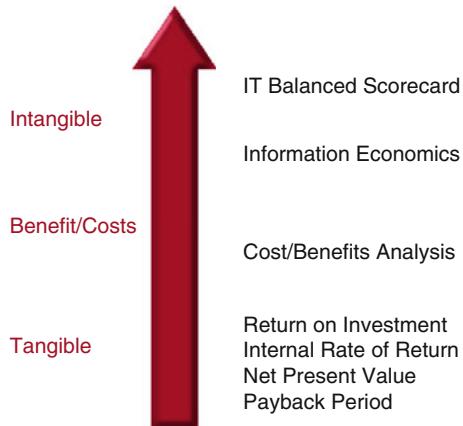
In the first place, the internal domain of the extended Strategic Alignment Model of Maes is subdivided into two separate areas: a structural and an operational level. This results from the observation that the former plays an essential role in the tuning of long-term strategic vision (which is set in the external domain) and the latter serves the short-term operational transformation. The IT domain in turn is being reshaped into an information/communication level and a technology level. The split of the IT domain results from the observation that most information and communication processes are IT independent and therefore need to be regarded separately. In this context, reference needs to be made to another new concept that is emerging in the field, under the name Information Governance, stating that it is all in the first place about the information and not the technology. The previous argumentation results in a 3×3 matrix as opposed to the 2×2 matrix first presented by Henderson and Venkatraman.

A very good and comprehensive literature review on alignment was published by Chan and Reich in the Journal of Information Technology (2007), titled: “IT alignment: what have we learned?” This is certainly a recommended reading material for both researchers and practitioners in this area.

1.3 Value from IT

A crucial question in the alignment debate is why the notion is so fundamentally important to an organization’s success. Much research has been conducted on this issue, particularly with a view to demonstrating the correlation between business/IT

Fig. 1.4 Performance measurement approaches



alignment and business performance. Chan and Reich (2007) categorize alignment as one of the important antecedents for organizational performance, based on studies of among other Bergeron et al. (2003), Chan et al. (1997), and Sabherwal and Chan (2001) that indeed confirm the hypothesis that alignment between business and IT strategies improves (perceived) business performance.

Above studies suggest that the alignment construct is an important intermediate variable or catalyst for business value creation from IT investments, though it remains a challenge how to demonstrate this IT-enabled value creation. There are different instruments available aimed at identifying and quantifying IT costs and IT benefits. When both costs and benefits can be easily quantified and assigned a monetary value, traditional performance measures such as ROI, net present value, internal rate of return, and payback method work well (Fig. 1.4).

Because the traditional methods need monetary values, problems emerge when they are applied to information systems, which often generate intangible benefits such as “better customer service” or “improved decision making.” Moreover, different levels of management and users perceive the value of IT differently. Broadbent and Weill (1998) refer in this context to the “business value hierarchy” (Fig. 1.5). Very successful investments in IT have a positive impact on all levels of the business value hierarchy. Less successful investments are not strong enough to impact the higher levels and consequently influence only the lower levels. The higher one goes in the measurement hierarchy, the more dilution that occurs from factors such as pricing decisions and competitors’ moves. This dilution means that measuring the impact of an IT investment is much easier at the bottom of the hierarchy than at the top.

Multicriteria measurement methods may solve this problem because they account for both tangible and intangible impacts, where the latter are more typical for the higher business value hierarchies. One of the best known multicriteria methods is information economics (IE), developed by Benson and Parker (1989) which in essence is a scoring technique whereby a mix of tangible benefits (typically ROI) and intangible benefits and risks are scored.

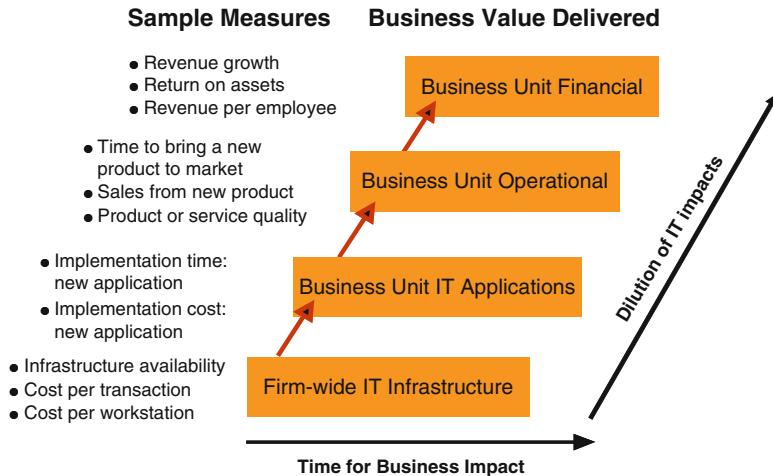


Fig. 1.5 Business value hierarchy. Adapted from: Broadbent, M., & Weill, P., 1998, Leveraging the new infrastructure—How market leaders capitalize on Information Technology, Boston, Massachusetts: Harvard Business School Press

A broader performance measurement technique is the BSC, which can be applied to IT projects, investments, and even entire IT departments. The BSC, initially developed on the enterprise level by Kaplan and Norton (1996), is a performance management system that enables businesses to drive strategies based on measurement and follow-up. The idea behind the BSC is that the evaluation of a firm should not be restricted to the traditional financial measures but should be supplemented with a mission, objectives and measures regarding customer satisfaction, internal processes, and the ability to innovate and prepare for the future. Results achieved within the additional perspectives should assure financial results. The objectives and measures of a BSC can be used as a cornerstone of a management system that uncovers and communicates strategies, establishes long-term strategic targets, aligns initiatives, allocates long- and short-term resources, and finally provides feedback and learning about the strategies. This application of the balanced scorecard on the IT related discussion will be addressed in Chap. 4.

Summary

Given the centrality of IT for enterprise risk management and value generation in digitized organizations, a specific focus on EGIT has arisen over the last two decades.

EGIT addresses the definition and implementation of processes, structures, and relational mechanism that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of value from IT-enabled business investments.

EGIT is an important enabler for business/IT alignment. Business/IT alignment is a complex construct as defined by Henderson and Venkatraman in 1993. This models stress the importance of balancing business and IT strategic and operational issues to obtain alignment.

Achieving a high degree of business/IT alignment in turn will enable the achievement of business value from IT. IT by itself will not generate value for the business. Value will only be realized with both IT and the business involved (aligned). The challenge still remains to measure and demonstrate the value of IT. For this, advanced approaches can be leveraged such as applying the balanced scorecard technique to measure and manage the value creation out of IT-enabled investments.

Study Questions

1. Define EGIT and explain the shift from IT Governance towards EGIT.
2. Explain and discuss the components of the concept of business/IT alignment.
3. Discuss why alignment can be difficult to achieve in organizations.
4. Explain the concept of “IT-enabled value” and discuss why it is difficult to demonstrate.
5. Describe and discuss the relationship between EGIT, alignment, and value creation.

References

- Benson, R., & Parker, M. (1989). Enterprisewide information economics: Latest concepts. *Journal of Information Systems Management*, 6(4), 7–13.
- Bergeron, F., Raymond, L., & Rivard, S. (2003). Ideal patterns of strategic alignment and business performance. *Information & Management*, 41(8), 1003–1020.
- Broadbent, M., & Weill, P. (1998). *Leveraging the new infrastructure—How market leaders capitalize on Information Technology*. Boston: Harvard Business School Press.
- Carr, N. G. (2003). IT doesn't matter. *Harvard Business Review*, 81(5), 41–49.
- Chan, Y., Huff, S., Barclay, D. W., & Copeland, D. W. (1997). Business strategic orientation, information systems strategic orientation, and strategic alignment. *Information Systems Research*, 8(2), 125–150.
- Chan, Y. E., & Reich, B. H. (2007). IT alignment: What have we learned? *Journal of Information Technology*, 22, 297–315.
- 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.
- De Haes, S., Van Grembergen, W., & Debreceny, R. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, 27, 1.
- Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM systems journal*, 32(1), 4–16.
- Hirt, M., & Wilmott, P. (2014). Strategic principles for competing in the digital age. *McKinsey Quarterly*, May 2014, 1–13.
- ISACA. (2007). *COBIT 4.1*. Retrieved from www.isaca.org

- ISACA. (2008). *VALIT*. Retrieved from www.isaca.org
- ISACA. (2009). *RISKIT*. Retrieved from www.isaca.org
- ISACA. (2012). *COBIT 5*. Retrieved from www.isaca.org
- ISO/IEC. (2008). *38500:2008—Corporate Governance of Information Technology*. Retrieved from www.iso.org
- Kaplan, R., & Norton, D. (1996). *The balanced scorecard: Translating vision into action*. Boston: Harvard Business School Press.
- Maes, R. (1999). *Reconsidering information management through a generic framework*. PrimaVera Working Paper 99-15.
- Sabherwal, R., & Chan, Y. (2001). Alignment between business and IS strategies: A study of prospectors, analyzers and defenders. *Information Systems Research*, 12(1), 11–33.
- Thorp, J. (2003). *The information paradox*. New York: McGraw-Hill.
- Van Grembergen, W. (2002). Introduction to the minitrack: IT governance and its mechanisms. In *Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS)*, Hawaii.
- Weill, P., & Ross, J. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Boston: Harvard Business School Press.
- Wilkin, C. L., & Chenhall, R. H. (2010). A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems*, 24(2), 107–146.
- Wu, S. P.-J., Straub, D. W., & Liang, T.-P. (forthcoming). How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. *MIS Quarterly*.

Chapter 2

Enterprise Governance of IT

Abstract The previous chapter provided a high-level description what Enterprise Governance of IT is about. However, having developed a high-level model for Enterprise Governance of IT does not imply that governance of enterprise IT is actually working in the organization. Conceiving the model for Enterprise Governance of IT is the first step, deploying it throughout all levels of the organization is the next challenging step. To achieve this, Enterprise Governance of IT can be deployed using a mixture of various structures, processes, and relational mechanisms. These practices will be discussed in this chapter, including an illustration how they were leveraged in the context of a large international airline company. Also, specific topics will be discussed such as the role of the board in enterprise governance of IT and the challenge of approaching enterprise governance of IT in an interorganizational context. Finally, a more theoretical view on enterprise governance of IT is discussed through the lens of the Viable Systems Model Theory.

2.1 Practices for Implementing Enterprise Governance of IT

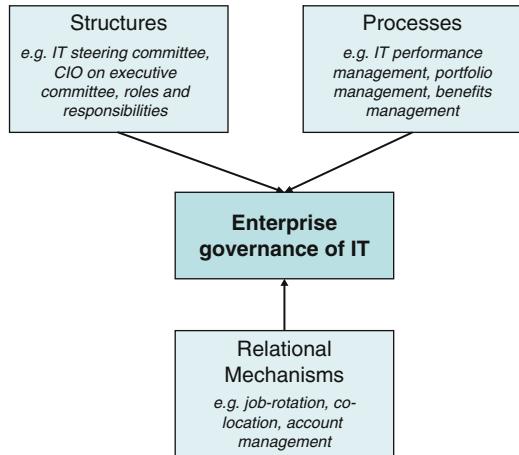
Having developed a high-level model for enterprise governance of IT does not imply that governance is actually working in the organization. Conceiving the enterprise governance of IT model is the first step, implementing it into a sustainable solution is the next challenging step. Our research (De Haes and Van Grembergen, 2009; Van Grembergen, 2004) showed that organizations can and are deploying enterprise governance of IT by using a holistic mixture of various structures, processes, and relational mechanisms.

Enterprise governance of IT structures include organizational units and roles responsible for making IT decisions and for enabling contacts between business and IT management decision-making functions (e.g., IT steering committee). This can be seen as a kind of blueprint of how the governance framework will be structurally organized.

Enterprise governance of IT processes refers to the formalization and institutionalization of strategic IT decision-making and IT monitoring procedures, to ensure that daily behaviors are consistent with policies and provide input back to decisions (e.g., portfolio management).

The relational mechanisms finally are about the active participation of, and collaborative relationship among, corporate executives, IT management, and business

Fig. 2.1 Structures, processes, and relational mechanisms for IT governance



management and include job-rotation, announcements, advocates, channels, and education efforts. Some examples of these structures, processes, and relational mechanisms are provided in Fig. 2.1.

In the many case organizations we visited (De Haes and Van Grembergen, 2009; De Haes et al., 2011), we saw that most organizations are indeed leveraging a mix of structures, processes, and mechanisms. Of course, it should be noted that a “silver bullet approach” does not exist in this matter. Each organization has to select its own set of enterprise governance of IT practices, suitable for their sector, size, culture, etc.

Our case research clearly showed that organizations tend to find it much easier to implement structures in their organizations as opposed to processes. However, we have also seen that many of these structures cannot be effective without supporting processes. For example, an IT steering committee cannot make appropriate investment decisions without an appropriate and mature portfolio management process, including the development of solid business cases. It also appeared that relational mechanisms, such as training, awareness building, etc., receive a lot of attention in the beginning stages of an enterprise governance of IT implementation project and become less important when the governance framework gets embedded into day-to-day operations. This is not surprising as the introduction of an approach towards enterprise governance of IT should be regarded in the first place as a large change programme within the organization.

Another interesting finding to pinpoint is that our enterprise governance of IT definition implies a prime responsibility of the board of directors (as part of their corporate governance responsibility), while specific mechanisms to achieve this such as “IT expertise at level of board of directors” are less existent in organizations (see separate Sect. 2.3 on this matter). This can possibly be explained by the fact that making the board of directors more IT literate is not easy to achieve, or that the board is still not fully aware of the strategic importance of IT.

More recently, the idea of “IT leadership” emerged in many discussion fora. IT leadership can be defined as the ability of the CIO or similar role to articulate a vision for IT’s role to the company and ensure that this vision is clearly understood by managers throughout the organization. If the CIO is not able to talk in business-oriented terms at executive level, his impact at that level will be small. This mechanism is highly

dependent on the individual competencies of the CIO and not many methods are available to manage it. However, we have seen that good leadership can be a very powerful catalyst to bring enterprise governance of IT in an organization to a next level. A good balance between leadership and the appropriate governance structures and processes needs to be found (De Haes and Van Grembergen, 2009).

To better understand how organizations can implement enterprise governance of IT, we have supplemented our case research with Delphi research, leveraging an expert panel of academics, business and IT managers and consultants, to try to inventorize and evaluate structures, processes, and relational mechanisms that contemporary organizations are using in implementing enterprise governance of IT (De Haes and Van Grembergen, 2009). This exercise resulted in a list of 33 enterprise governance of IT practices, and their respective evaluations in terms of perceived effectiveness and perceived ease-of-implementation (see Fig. 2.2). Based on their answers regarding perceived effectiveness, also a minimum baseline was constructed, as a list of practices that organization at least should have. After several review rounds, the expert panel categorized these ten practices indicated in bold as key instruments for enterprise governance of IT (Fig. 2.2).

This minimum baseline (in bold) contains a mixture of more strategic-oriented (e.g., IT strategy committee at level of board of directors) and management-oriented (e.g., IT project steering committee) practices. It is also clear that practices such as IT steering committee, portfolio management, and project governance/management constitute the core framework to describe how investments in organizations emerge are prioritized and realized. In that sense, most of the practices above clearly contain both business and IT-oriented roles and responsibilities.

Assignment Box 2.1: IT Steering Committee Charter

You are working for an international bank and the CEO has asked you to create a charter for a new IT steering committee. Using the template below, provide a description of how you see the role, responsibility, participants, and frequency of meetings. Be prepared to defend your solution.

IT Steering Committee - Charter

• Role

• Responsibility (decision power)

• Frequency

• Participants

Assignment Box 2.2: Assessment of Enterprise Governance of IT Practices

If you have access to an organization, assess the presence and maturity of the enterprise governance of IT practices as discussed in this section. You can use the template below, each time indicating whether the practice is not present (0) versus very mature (5) and providing a corresponding rationale. You can also add other practices in the list that where not discussed in this chapter.

	Organisation	
	Maturity	Rationale
IT strategy committee at level of board of directors	0 / 1	2 / 3 / 4 / 5
IT expertise at level of board of directors	0 / 1	2 / 3 / 4 / 5
(IT) audit committee at level of board of directors	0 / 1	2 / 3 / 4 / 5
IT executive committee	0 / 1	2 / 3 / 4 / 5
CIO reporting to CEO and/or COO	0 / 1	2 / 3 / 4 / 5
IT steering committee (IT) investment evaluation / prioritisation at executive / senior management level/012345	0 / 1	2 / 3 / 4 / 5
IT governance function / officer	0 / 1	2 / 3 / 4 / 5
Security / compliance / risk officer	0 / 1	2 / 3 / 4 / 5
IT project steering committee	0 / 1	2 / 3 / 4 / 5
IT security steering committee	0 / 1	2 / 3 / 4 / 5
Architecture steering committee	0 / 1	2 / 3 / 4 / 5
Integration of governance/alignment tasks in roles&responsibilities	0 / 1	2 / 3 / 4 / 5
Strategic information system's planning	0 / 1	2 / 3 / 4 / 5
IT performance measurement (e.g. IT balanced scorecard)	0 / 1	2 / 3 / 4 / 5
Portfolio management (incl. business cases, information economics, ROI, payback)/012345	0 / 1	2 / 3 / 4 / 5
Charge back arrangements - total cost of ownership (e.g. activity based costing)	0 / 1	2 / 3 / 4 / 5
Service level agreements	0 / 1	2 / 3 / 4 / 5
IT governance framework COBIT	0 / 1	2 / 3 / 4 / 5
IT governance assurance and self-assessment	0 / 1	2 / 3 / 4 / 5
Project governance / management methodologies	0 / 1	2 / 3 / 4 / 5
IT budget control and reporting	0 / 1	2 / 3 / 4 / 5
Benefits management and reporting	0 / 1	2 / 3 / 4 / 5
COSO / ERM	0 / 1	2 / 3 / 4 / 5
Job-rotation	0 / 1	2 / 3 / 4 / 5
Co-location	0 / 1	2 / 3 / 4 / 5
Cross-training	0 / 1	2 / 3 / 4 / 5
Knowledge management (on IT governance)	0 / 1	2 / 3 / 4 / 5
Business/IT account management	0 / 1	2 / 3 / 4 / 5
Executive / senior management giving the good example	0 / 1	2 / 3 / 4 / 5
Informal meetings between business and IT executive/senior management	0 / 1	2 / 3 / 4 / 5
IT leadership	0 / 1	2 / 3 / 4 / 5
Corporate internal communication addressing IT on a regular basis	0 / 1	2 / 3 / 4 / 5
IT governance awareness campaigns	0 / 1	2 / 3 / 4 / 5
Other practices	0 / 1	2 / 3 / 4 / 5
General remarks		

A generic indication of the maturity scale is provided below. To make the analysis in-depth, the scale should be made specific for each of the practices (e.g., what do you expect if portfolio management is at level 5).

0. Nonexistent: There is a complete lack of any recognizable IT Governance practice.
1. Initial/ad hoc: The organization has recognized that IT Governance issues exist and need to be addressed.
2. Repeatable but intuitive: There is awareness of IT Governance objectives, and practices are developed and applied by individual managers.
3. Defined: The need to act with respect to IT Governance is understood and accepted. Procedures have been standardized, documented, and implemented.
4. Managed and measurable: IT Governance evolves into an enterprise-wide practice and IT Governance activities are becoming integrated with the enterprise governance process.
5. Optimized: Enterprise governance and IT Governance are strategically linked, leveraging technology and human and financial resources to increase the competitive advantage of the enterprise.

	Index	IT governance practice	Definition
IT governance structures	S1	IT strategy committee at level of board of directors	Committee at level of board of directors to ensure IT is regular agenda item and reporting issue for the board of directors
	S2	IT expertise at level of board of directors	Members of the board of directors have expertise and experience regarding the value and risk of IT
	S3	(IT) audit committee at level of board of directors	Independent committee at level of board of directors overviewing (IT) assurance activities
	S4	CIO on executive committee	CIO is a full member of the executive committee
	S5	CIO (Chief Information Officer) reporting to CEO (Chief Executive Officer) and/or COO (Chief Operational Officer)	CIO has a direct reporting line to the CEO and/or COO
	S6	IT steering committee (IT investment evaluation / prioritisation at executive / senior management level)	Steering committee at executive or senior management level responsible for determining business priorities in IT investments.
	S7	IT governance function / officer	Function in the organisation responsible for promoting, driving and managing IT governance processes
	S8	Security / compliance / risk officer	Function responsible for security, compliance and/or risk, which possibly impacts IT
	S9	IT project steering committee	Steering committee composed of business and IT people focusing on prioritising and managing IT projects
	S10	IT security steering committee	Steering committee composed of business and IT people focusing on IT related risks and security issues
	S11	Architecture steering committee	Committee composed of business and IT people providing architecture guidelines and advise on their applications.
	S12	Integration of governance/alignment tasks in roles & responsibilities	Documented roles & responsibilities include governance/alignment tasks for business and IT people (cf. Weill)
IT governance processes	P1	Strategic information systems planning	Formal process to define and update the IT strategy
	P2	IT performance measurement (e.g. IT balanced scorecard)	IT performance measurement in domains of corporate contribution, user orientation, operational excellence and future orientation
	P3	Portfolio management (incl. business cases, information economics, ROI, payback)	Prioritisation process for IT investments and projects in which business and IT is involved (incl. business cases)

Fig. 2.2 Practices for enterprise governance of IT

IT governance relational mechanisms	P4	Charge back arrangements - total cost of ownership (e.g. activity based costing)	Methodology to charge back IT costs to business units, to enable an understanding of the total cost of ownership
	P5	Service level agreements	Formal agreements between business and IT about IT development projects or IT operations
	P6	IT governance framework COBIT	Process based IT governance and control framework
	P7	IT governance assurance and self-assessment	Regular self-assessments or independent assurance activities on the governance and control over IT
	P8	Project governance / management methodologies	Processes and methodologies to govern and manage IT projects
	P9	IT budget control and reporting	Processes to control and report upon budgets of IT investments and projects
	P10	Benefits management and reporting	Processes to monitor the planned business benefits during and after implementation of the IT investments / projects.
	P11	COSO / ERM	Framework for internal control
	R1	Job-rotation	IT staff working in the business units and business people working in IT
	R2	Co-location	Physically locating business and IT people close to each other
	R3	Cross-training	Training business people about IT and/or training IT people about business
	R4	Knowledge management (on IT governance)	Systems (intranet, ...) to share and distribute knowledge about IT governance framework, responsibilities, tasks, etc.
	R5	Business/IT account management	Bridging the gap between business and IT by means of account managers who act as in-between
	R6	Executive / senior management giving the good example	Senior business and IT management acting as "partners"
	R7	Informal meetings between business and IT executive/ senior management	Informal meetings, with no agenda, where business and IT senior management talk about general activities, directions, etc. (e.g. during informal lunches)
	R8	IT leadership	Ability of CIO or similar role to articulate a vision for IT's role in the company and ensure that this vision is clearly understood by managers throughout the organisation
	R9	Corporate internal communication addressing IT on a regular basis	Internal corporate communication regularly addresses general IT issues.
	R10	IT governance awareness campaigns	Campaigns to explain to business and IT people the need for IT governance

Fig. 2.2 (continued)

2.2 Principles for Enterprise Governance of IT

In practice, organizations often try to express a number of “principles,” which clearly state how business and IT will collaborate in the organization. These principles are to be defined jointly by business and IT and constitute a kind of contract between business and IT. These are often a good starting point to use as reference when building enterprise governance of IT structures, processes, and relational mechanisms.

Examples of principles used in real-life organizations are provided in Fig. 2.3. Each of these principles of course require more detailed definitions and descriptions of what exactly the implications are towards required structures, processes, and relational mechanisms. In that sense, such principles become the starting point to “design” and appropriate model for enterprise governance of IT. In Sect. 2.3, an illustration is provided how such principles can be translated towards required enterprise governance of IT structures, processes, and relational mechanisms.

- IT is a professional organization that effectively and efficiently manages its resources in alignment with the needs of the organization.
- IT is the exclusive provider of IT services. Outsourcing is always organised in joint partnership between business and IT.
- IT is proactively engaged in further developing and innovating the organization.
- IT primarily develops and maintains competencies that are aligned to and required for supporting the expertise available in the organization.
- The priorities within IT are aligned to the strategic goals of the organization through integrated planning cycles.
- All IT applications comply with rules and policies as mutually agreed upon by business and IT
- IT is proactively engaged in reviewing and designing efficient business processes.
- IT and the business collaborate based on fixed agreements. Based on a scope definition, impact analysis and capacity reviews, both business and IT commit for timely delivery within quality requirements.
- There is transparency on the required service quality that IT has to deliver to the business, and this service quality is continuously monitored.
- Starting from the initial development of a new business project, the potential impact on IT needs to be analysed.

Fig. 2.3 Enterprise governance of IT principles

Assignment Box 2.3: Understanding Enterprise Governance of IT Principles

Discuss in group the meaning of the Enterprise Governance of IT principles as depicted in Fig. 2.3. Describe which structures, processes, and relational mechanisms you would propose to design an enterprise governance of IT model that allows these principles to be realized in the organization. Present and discuss the results to the class.

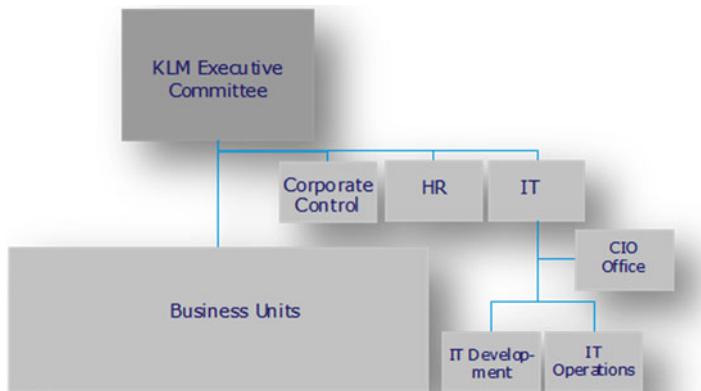


Fig. 2.4 Organizational structure of KLM

2.3 Case Study: Enterprise Governance of IT at KLM

The airline company KLM was founded in 1919, and has its home base and hub in Amsterdam Schiphol Airport (Netherlands). KLM currently employs over 33,000 people worldwide, and manages a fleet of about 200 aircraft. In 2004, KLM merged with Air France, after which both companies continued to operate as separate airlines, each with their own identity and brand, and each benefiting from each other strengths. In financial turnover, Air France-KLM is the world's largest airline group, transports the most passengers and is the world's second largest cargo transporter. In 2009, Air France-KLM operated flights to 255 destinations in 115 countries on 4 continents.

This case focuses on the KLM activities within the Air France-KLM group. The KLM Executive Committee (Fig. 2.4) is composed of the CEO, CFO, Managing Director, and all Executive Vice Presidents (EVP) of the major business units and services (Commercial, In-flight Services, Operations, Ground Services, Cargo, Engineering & Maintenance, IT and HR). In 2009/2010, KLM IT employed close to 1,000 (internal and external) FTEs, with an IT budget of around 300 million euro. As shown in Fig. 2.4, KLM IT is organized around IT development activities, IT operations activities, and the CIO-Office addressing aspects of the enterprise/IT

architecture, IT strategy, value and portfolio management, sourcing strategy, and risk & security. The mission of the IT department is to “create business value by delivering reliable IT services to the business processes, and innovative IT solutions to enable and support business changes.” The following strategic goals for IT support this mission:

- IT is a world class Information Services provider and will be able to deliver the best value to the company
- The IT cost-levels will be at a competitive industry level
- The IT architecture and infrastructure will enable the growth ambitions of Air France-KLM

2.3.1 KLM’s Trigger Points to Start the Journey

IT is a business-critical enabler for KLM yet, at the same time, can be a source of both success and discontent. In 2001, the balance had tilted towards discontent due to a lack of trust in what was perceived as a very costly and unresponsive IT department. This, in a business climate that was increasingly challenging, and which became dramatically more so after the 9/11 terrorist attacks. After that event, KLM’s CEO seized the opportunity to make a structural break with the past, and reexamine and transform KLM’s business and IT governance.

The Executive Vice President (EVP) of the Operations Control Centre was appointed as new CIO. It was felt that having the CIO coming out of the “real business” would help in getting the “IT governance” discussion out of the IT area, and have it put on the business executive’s agenda. The newly appointed CIO received three clear priorities:

1. Provide the reasons why, or why not, to outsource IT;
2. Create a business/IT board to organize joint success; and
3. Design simple governance principles to restore control enabling steering by the Executive Vice Presidents (EVPs) and the CIO.

In order to respond to these requirements, the CIO-Office was established as a support function to the CIO, consolidating a number of already existing, loosely coupled, and different functions such as an IT Strategy Office, Programme Management, and business/IT liaison roles. In the words of the Vice President (VP) of the CIO-Office: “In the scenario that we would outsource IT, both IT operations and development would mainly be sourced outside KLM, but the activities of the CIO-Office would be kept internally, as it governs IT strategy, architecture, security, business/IT alignment, etc. The goal of the CIO-Office is to enable effective IT, in support of business needs.”

2.3.2 Embarking on the Journey

It was decided that, ahead of the first priority stated above, the primary focus should be to introduce better governance principles and practices (priority 3). A project under the title “IT: A Collaborative Effort” was launched, focused at enabling all stakeholders to better understand the cost and value of IT, which in turn would enable them to make more informed decisions on what and how to potentially outsource (priority 1). In support of priority 2, a business/IT board was established, composed of the CEO, CIO, and all business units EVPs, meeting every quarter to discuss and decide on strategic issues involving IT.

With regard to priority 3, the CIO-Office, in collaboration with the business, designed a set of principles that would significantly simplify IT-related governance. The starting premise was that these principles should put the business in full control of all IT demand and IT spend. In support of these principles, a number of governance practices were introduced in the business and IT organizations, including the establishment of the business/IT board and demand management functions for each business domain. These governance principles and practices were introduced as “the only way of working” between business and IT for all business units and activities. These practices also supported the creation of portfolio management processes driven by the business units. The portfolio management processes evolved from being IT resource- and supply-driven towards business demand-driven with an innovative and rigorous approach to evaluation and selection.

2.3.2.1 Governance Principles and Practices

The definition of the first draft set of governance principles and practices was mainly driven by the CIO-Office. These principles were later refined with the involved business parties and are now shared in the organization through the intranet. According to the Director Value Management & Alliances (member of the CIO-Office): “These principles and practices are still challenged from time to time. Our position is that we are always open for discussion for each of these principles and practices, but up till now, we have each time in the end reconfirmed them.” The stated principles and practices apply for all business units and are presented in internal KLM presentations as shown in Fig. 2.5. The involved parties acknowledge that this list does not really distinguish between principles and practices and presents them in a mixed way, but it was felt to be a pragmatic and practical list that was workable for KLM. The CIO-Office developed more detailed background information and internal documentation to explain the impact and consequences of each of these principles and practices.

The first key principle (1) states that, for the business, there should be no difference in dealing with an internal or external IT provider. This recognizes that business should be in full control of all IT demand and IT spend (supply). Related to the latter, criteria were developed regarding choosing between allocating work in-house for

1. For the business there should be no difference between working with an internal or external IT-provider.
2. Differentiate between WHAT and HOW (and WHY).
3. Improve the Demand-function by creating a Business Demand Office per business domain.
4. Improve the Supply function by creating an Innovation Organizer and a Service Manager per business domain.
5. Create monthly decision meetings of What and How (management and IT).
6. Focus on the cost that can be influenced in full and those that can be influenced in part: Split between Innovation and Continuity.
7. Each Innovation (investment) has one business owner to which all cost are charged.
8. Each Service (Continuity) has one business owner to which all cost are charged.
9. Top-down budget framework and simplified budget process.
10. Activity-Based Costing applied to process primary cost to product cost.

Fig. 2.5 Principles for enterprise governance of IT at KLM

customized development, or through external IT providers for standardized solutions. These “selective sourcing” agreements are internally referenced as the “Stay on the Surfboard Principle” (Fig. 2.6). Generic business processes that bring no competitive advantage (such as office support, collaboration, and payroll) will be supported by generic (low development cost, off-the-shelf) applications packages. Business processes, which have the potential to create competitive advantage (such as CRM, revenue management), can and will be supported by in-house (higher development cost) custom-built applications. The VP CIO-Office explains: “In the past, we evolved to a situation where many commodity services were built and maintained in-house, when businesses were only interested in a good service at low cost for these mainstream applications. The surfboard helped in the discussions on what and what not to outsource, and to bring the debate on ‘we want more IT for less money’ to another level, oriented towards ‘we need different IT for different businesses’.”

The next set of principles and practices (2–5) define a clear split between IT-related activities in terms of the WHAT-activities and HOW-activities, or in other terms between Demand and Supply. Before 2001, IT demand came in via 14 Information Management committees and numerous informal channels. According to the VP CIO-Office: “In the old situation, demand came in through too many different channels, and there was no coordination between those channels. For example, it could be that five similar investment requests were put forward, initiated from different business lines.” “Moreover,” as reinforced by the Director Value

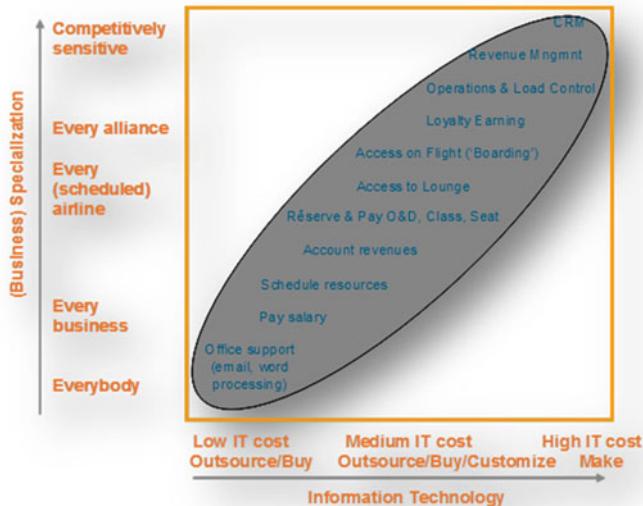


Fig. 2.6 Surfboard principle for outsourcing

Management & Alliances, “some of the Information Management groups also managed a separate IT development team, leading to a very scattered approach.” To improve the demand function, all business demand for investments and innovation is now channelled via Business Demand Offices (BDOs) for the five business domains of KLM (Engineering and Maintenance, Cargo, Passenger Commercial, Passenger Operations, Corporate).

These BDOs are formally positioned in the business department in close contact with their EVPs and with a reporting line to the CIO. Commenting on this, the VP Finance and Control Ground Services says: “Putting the BDOs directly in the business was a very important governance design decision, as it enabled them to really act as business representatives.” Each BDO has a dedicated counterpart or mirror-role on the IT supply side, called the “Innovation organizer,” responsible for all HOW-activity (see Fig. 2.7). Realizing this split was a challenge, as the VP CIO-Office explains: “This clear distinction between demand and supply seems obvious, but it implied a huge effort in terms of company meetings, consultations and moving people.”

As stated in principle 6, a clear differentiation is established between the innovation cost that can be fully influenced by the business, and the continuity cost (running cost to “keep the lights on”) that can only be partly influenced. The innovation budget includes all manpower, purchases, work-by-3rd-parties, and other out-of-pocket project cost required to build new IT services and functional changes to existing IT services (“enhancements”). The BDOs register agreed “innovation” work on the basis of which the Innovation Organizer coordinates IT development,

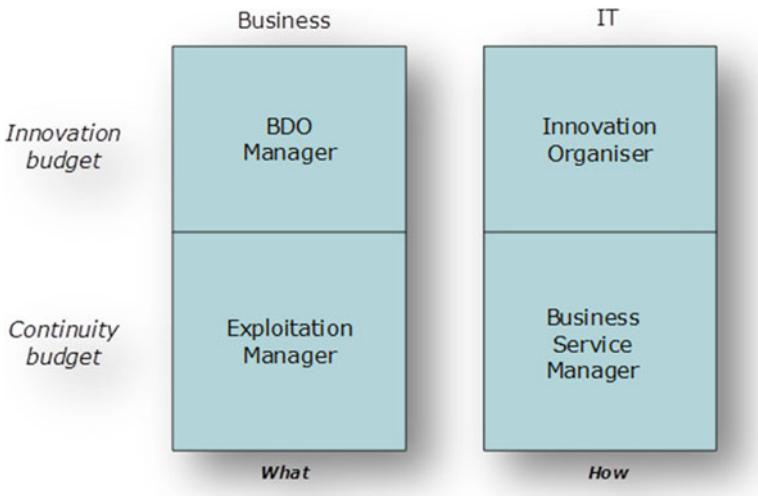


Fig. 2.7 Mirror roles between business and IT

time-accounting, and charge-out. The continuity budget includes cost for IT services, desktops, data communication, and telecommunication and is managed, in terms of volume and quality, by the “exploitation manager” on business side, together with the “business service manager” on IT supply side (see Fig. 2.7). The objective of these business service managers is to deliver continuity of the KLM operations in an efficient way and at lowest IT cost.

This split between the innovation (programme) portfolio and the continuity (service) portfolio is internally explained with the image of “the bicycle” (Fig. 2.8). This “bicycle” is mainly used as a visual aid to internally communicate at a high and conceptual level the split and relationship between the continuity and innovation budget. As visualized, the business/IT strategy drives the definition and application of the governance principles and priority rules and the definition of business cases. The approved business cases are managed in the programme (innovation cycle), which, after delivery, become operational services being deployed and administered in the service (continuity) portfolio. As a result of ongoing evaluation, services may continue with no change, reenter the innovation cycle through a new business case, or be eliminated (retired).

All these roles created different decision platforms for IT-related governance, as shown in Fig. 2.9. There are a number of scheduled activities, involving different stakeholders and occurring at different frequencies, which occur throughout the year:

- Twice a year the Group Executive Committee is updated on how IT will respond to new challenges and directions in the businesses.
- The CEO, CFO, CIO, and Business EVPs meet every 2 months in the Business/IT Board to discuss and decide on strategic planning related to IT, and approve the IT budget and portfolio of programmes.

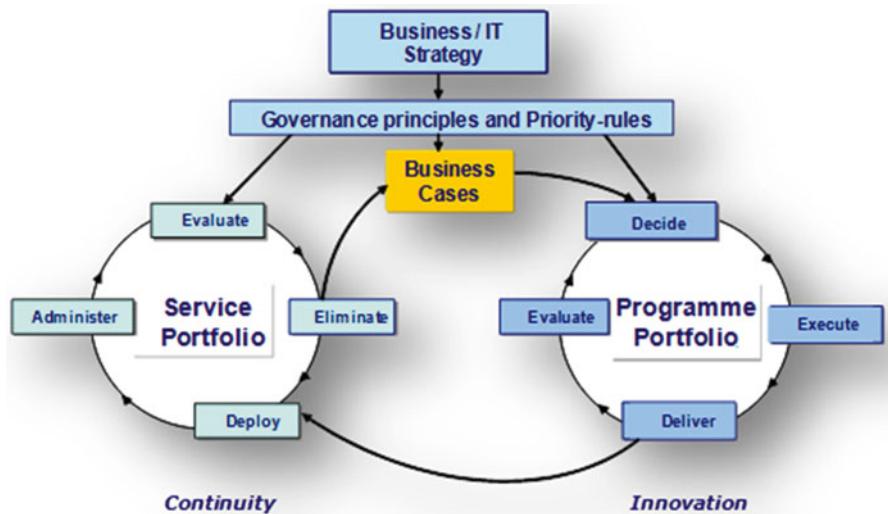


Fig. 2.8 The innovation-continuity bicycle

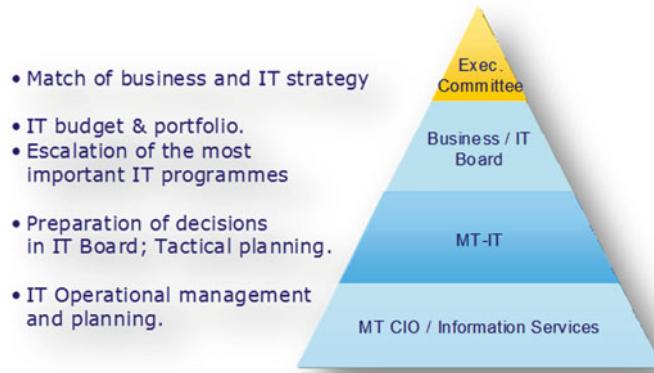


Fig. 2.9 Enterprise governance of IT decision platforms

- The Management Team of the IT provider plus the five BDOs meet monthly in the MT-IT, chaired by the CIO. They discuss and decide on tactical planning matters and prepare decisions for the business/IT board.
- Every 2 weeks the management team of Information Services meets to discuss and decide on operational and running issues.

To manage the demand of the IT function for infrastructure investments, business cases for which have traditionally been difficult to justify, a separate BDO for the IT department was created. The Director Finance and Control IT Operations argues: "If, for example, you have a storage technology which cannot be virtualized, you

may be able to build a business case to migrate to a new storage technology where virtualization is possible, resulting in lower business service costs. But for other infrastructure type investments, such as the migration of operating systems, the business case will be built on a risk avoidance and cost of future operational support.” The IT-BDO, part of the CIO-Office, analyzes future needs and capacity based on the incoming business cases of the businesses. Potential investments are then translated into an IT business case, and are discussed with the other BDOs in the “Information Security and Architecture Meeting” (ISAM). Once approved, the CIO-Office takes ownership to implement these infrastructure services. If possible, such investments are linked to other business investments that are being planned.

Principles 7–10 address the budgeting and cost accounting processes. The previous process of charging out IT costs to the business, with more than 3,300 technical cost components being charged to more than 3,400 cost account centers, was unwieldy, and provided little useful management information. The VP Finance & Control Ground Services concluded: “As a result, business perceived IT as a black box which they could not control, and therefore as something that was very likely to be too expensive.” Drastic simplification of the budgeting process was needed, essentially from charging hundreds of technical items to hundreds of departments of users, to charging only 7 products with associated cost: 2 for innovation and 5 for continuity, to 12 respective single/unique business owners (units). All budgets and costs (both continuity and innovation) are managed, forecasted, and made transparent through a cost portal, driven by activity-based costing principles, enabling clear and active ownership of the business of all IT-related costs.

2.3.2.2 Portfolio Management

The above governance principles and practices were needed as key building blocks in support of having effective portfolio management processes driven by the business units. The design of these portfolio management processes was done by the Portfolio Management Office (part of the CIO-Office) and is shown in Fig. 2.10. Three approval stages are defined, going from “idea selection” to “programme go” and “investment approval.” For each of these phases, clear decision thresholds were defined. For investments between 150,000 and 500,000 €, the EVP, Director Finance and Control and BDO of a business unit could approve the go/no-go decision in each phase, investments above 500,000 € are approved by the Business Unit Investment Committee (BIC), comprising the business unit COO, EVP, Director Finance and Control, and BDO and investments above 5,000,000 € are approved by the Executive Committee (EC).

The initial phase (1) addresses the initiation of the investment proposals or idea generation. In this phase, all business ideas are gathered and captured by the BDOs (demand process) and turned into potential initiatives for which a high-level business case (HLBC) will be developed. These HLBCs include descriptive information, classifications and high-level cost and benefits estimates and risk. The VP BDO Passenger Operations clarifies: “It is often hard to quantify some benefits at this stage. For example, the cost avoided of an aircraft not needing to land on



Fig. 2.10 Portfolio management process

another location because of better support systems. But still, we try to make as good as possible educated estimations.” If an initiative is approved (2), it is turned into a programme for which a full business case (BC) is developed based on a detailed feasibility study. To enable common and comparable business cases, a business case template was developed as a mandatory instrument for all investments above 150,000 €.

In order to be able to prioritize all these business cases, it is crucial to know what the organization’s business drivers are. The Director Value Management and Alliances makes clear: “Our experience was that it was often difficult to obtain a clear list of business priorities from a business unit. However, we needed these priorities to enable the selection of ‘the right things’ and for that reason we used a methodology to help us and the business in making these business priorities transparent.” The business drivers of a business unit are captured by the CIO-Office through interviews with the business unit executives. In the example of the Passenger Operations business unit, seven different business priorities were identified (see Fig. 2.11). Next, each of these business drivers are ranked through a pairwise comparison technique. Instead of just ranking the drivers from 1 to n , this technique relates each driver to the other drivers in terms of relative importance, ranging from “extremely less” toward “extremely more” in five sequential steps (e.g., “competitive unit cost” is relatively more important than “quality in physical comfort”). After completion of this pairwise comparison by each of the executive directors, a prioritized list of the defined business drivers is created and normalized into percentages that sum up to 100 % as shown in the Passenger Operations example below.

In the following step, the same pairwise comparison technique is used to determine the contribution of the investment proposals to each business driver. For each investment proposal the contribution to each of the business drivers is determined, ranging from “low” toward “extreme.” The result of these steps is an initial portfolio containing a ranked, but still unconstrained, list of all investment proposals at business unit level. The VP BDO Passenger Operations explains the importance of this process: “These

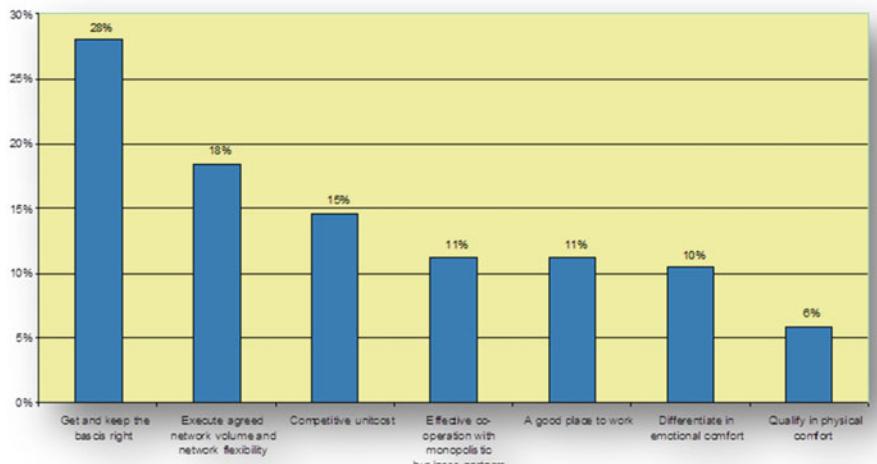


Fig. 2.11 Definition of the business drivers for passenger operations

priorities are the basis to build a ‘business plan’ for the BDO of a specific business unit, describing all the things that the BDO-office of a business unit can be held accountable for. I have even turned this business plan into a video clip on you-tube, to demonstrate to all our business and IT stakeholders our commitment for the next year.”

After this prioritization, total demand of all business units typically exceeds the budget made available by the executive committee. The Director Value Management and Alliances describes how this is handled: “Instead of using a ‘cheese slicer’ and, for example, forcing all business units to cut 30 % out of the project portfolio, a process of informal discussions is initiated between the BDOs to determine how the portfolio can best be optimized. As long as this process works, this approach is preferred instead of escalating to the next management level.” This process generally works well, and as a result, the business/IT board receives an overview of the major programmes and just has to endorse the outcome of the portfolio management process. The Director Value Management and Alliances concludes: “Through a good portfolio management process, we strive for seamless decision making.”

Once the portfolio of programmes is optimized, the business investment committee (for project above 500,000) or executive committee (for project above 5,000,000) still has to release the funding before design, construction, user acceptance testing (UAT), and implementation can start. This might appear as a duplicated decision structure, but it acts as a final check and it also gives the final authority and decision power back to the business executives. The VP BDO Passenger Operations explains: “In the end, the business executives decide. This approach helped in getting them engaged in the portfolio management process because they get their control back, although until now they have never ‘used’ it. Another important aspect in this context is that we try to make the time between the business idea and approval on the investment committee as short as possible, as this period is perceived as ‘IT being slow’.”

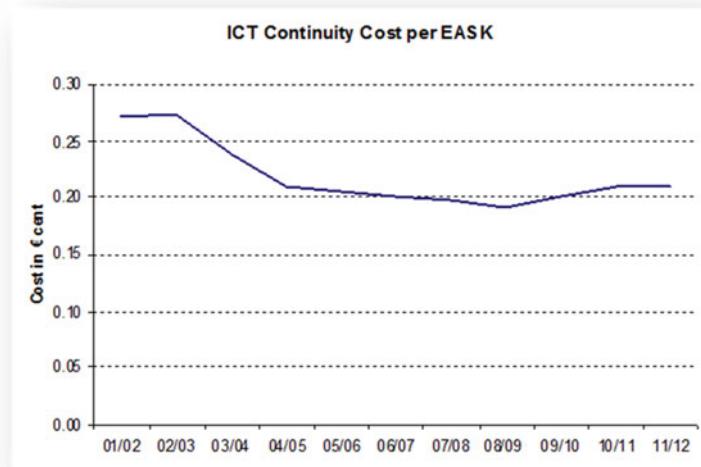


Fig. 2.12 IT continuity per business operation cost

2.3.3 *Reported Benefits*

During the interviews with the stakeholders in this case study, the following benefits of the improved enterprise governance of IT, which are discussed further in the following paragraphs, were consistently mentioned. They include:

- Lower IT continuity cost per business production unit
- Increased capacity for innovation
- Increased alignment of investments to strategic goals
- More trust between all involved stakeholders
- Moving beyond cost thinking towards a value culture

Lower IT continuity cost: A primary goal of the CIO-Office is to continuously promote, improve, and demonstrate the value of the enterprise governance of IT principles and practices in ensuring that IT-enabled investments contribute to real business value. In this effort, one of the metrics reported by the CIO-Office is the relation between all IT continuity costs and “Equivalent Available Seat Kilometers” (EASK), the key metric used to monitor airline production, which represents the total number of seats and cargo capacity multiplied by the total number of kilometers flown by the airline fleet. The graph below shows that although many business investments involving IT, such as e-Tickets, more web-based sales and web-based check-in, resulted in a year-on-year increase in the total IT budget, the unit cost of providing IT services (IT Continuity cost) per airline production unit decreased by more than 20 %. (The slight upward curve for the next 3 years is due to a temporary decrease of production in response to the world economic crisis.) This substitution of labour by IT also resulted in lower business cost per unit, since IT is cheaper than labour (Fig. 2.12).

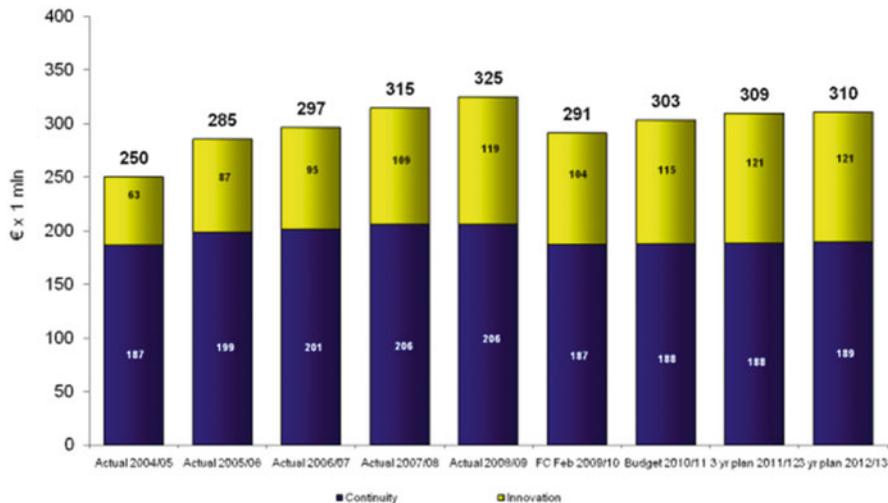


Fig. 2.13 IT continuity versus innovation budget

Increased innovation capacity: In addition to direct cost savings, the innovation capacity has increased as lower, or at least stable IT continuity costs contributed to freeing up financials for IT-based innovation. Again here, the CIO-Office develops metrics to demonstrate this outcome, of which one example is shown in Fig. 2.13. This bar chart shows a relative stable IT continuity budget, enabling the increase of the total IT budget to go almost entirely to new innovation, which has increased from 25 % in 2004/2005 to 39 % in 2010/2011.

Increased alignment of investments to strategic goals: The use of an innovative and inclusive process to capture and prioritize the business drivers of business units has enabled investment decisions to move beyond what was previously a fairly arbitrary process (in the case of cost reductions), or a largely subjective and emotional discussion (in the case of new innovations), to a more objective one. The new process, which involves discussions with and between business units and the CIO-Office, is based on contribution of existing or proposed spend to business drivers. It has resulted in increased alignment of investment and spend with business unit drivers and strategic goals, and increased confidence in the decision-making process. This increased confidence has also resulted in the business/IT board spending less time debating the merits of major programmes and generally endorsing the outcome of the portfolio management process.

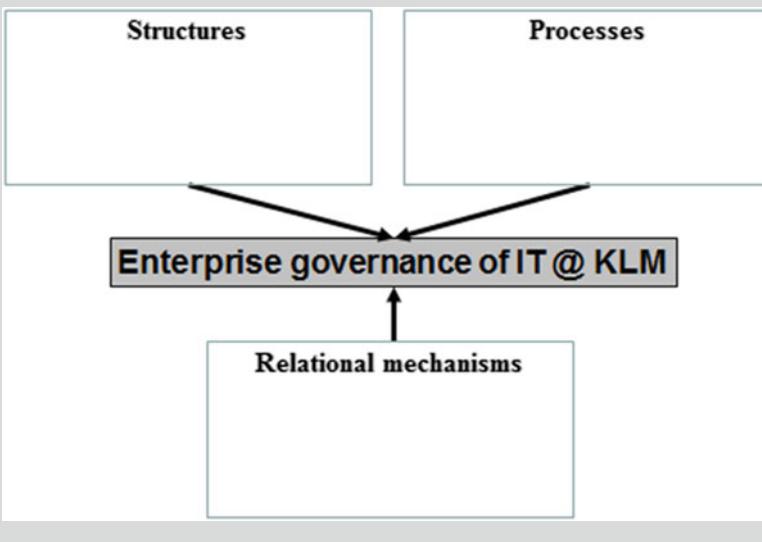
More trust: A fourth reported benefit is the increased trust between business and IT. The whole governance and portfolio management process has resulted in improved and more transparent decision-making. The results of the driver prioritization and investment contribution to the business strategy are visible for every

manager and stakeholder involved. It makes it difficult for executives to overvalue their own favorite proposals. Because of this, there is more trust, and this helps in continuing the “IT: a collaborative effort” journey.

A value culture: Finally, the process of managing the change towards improved enterprise governance of IT has its own benefits. The communication and discussions on portfolio management have improved management awareness and understanding, and supported the transformation from cost towards a value culture. It also continues to identify further opportunities to improve existing governance processes and practices.

Assignment Box 2.4: Identifying Practices for Enterprise Governance of IT

In the beginning of this chapter, Enterprise governance of IT is defined as an integral part of enterprise governance addressing 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. Revisit the case and identify the structures, processes, and relational mechanisms applied in this case. Make sure you can clearly explain each of these practices and its role in the context of enterprise governance of IT.



2.4 Enterprise Governance of IT and the Board

In the previous decade, there has been a lot of confusion in the market and literature in the use of the terminology “IT Management” versus “IT Governance.” As will be discussed in one of the following chapters on COBIT 5, ISACA has provided in 2012 a clear definition of both the concept and the difference between them. In building these definitions, ISACA has built on the position put forward by ISO/IEC 38500 (ISACA, 2012).

In COBIT 5, ISACA states that IT governance and IT management processes encompass different types of activities. The governance processes are organized following the EDM model (“Evaluate—Direct—Monitor”), as proposed by the ISO/IEC 38500 standard on Corporate Governance of IT (Fig. 2.14).

IT governance processes ensure that enterprise objectives are achieved by evaluating stakeholder needs (Evaluate), directing, and delegating decision-making roles, responsibilities, and processes in the organization (Direct); and monitoring performance, compliance, and progress against plans (Monitor). In enterprises, IT governance should be the accountability of the board of directors under the leadership of the chairperson. An example of such governance activity of the board can be that the board needs to understand and articulate the role of IT for the organization. A typical approach here is to have a discussion in the board that leads to an interpretation of the quadrant as proposed by Nolan and McFarlan (2005), and that the board takes the consequences of these choices. For example, if the board evaluates that their organization is highly depending on both new technology for innovation as on reliable technology for supporting running business activities, the organization is positioned in the “strategic mode” quadrant. In such scenario, it is up to the board

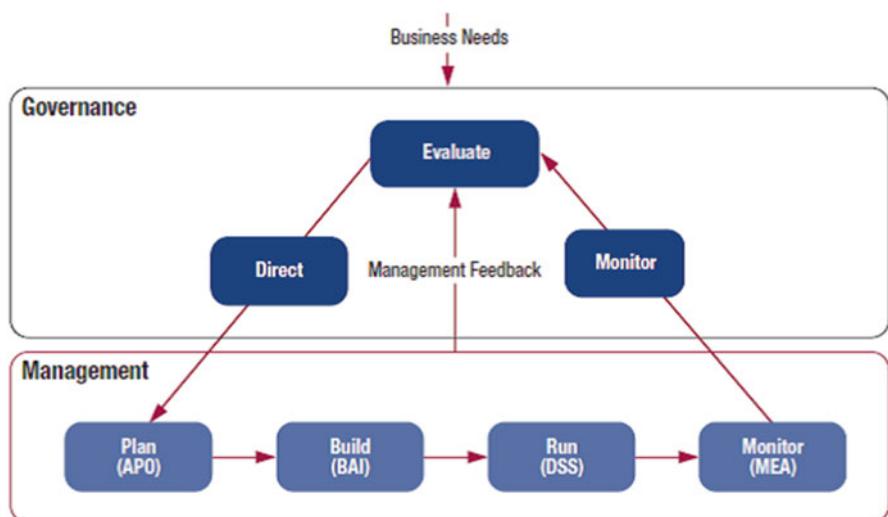
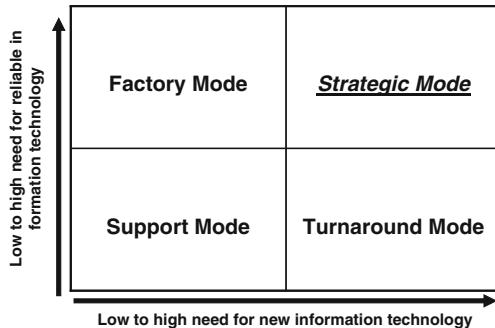


Fig. 2.14 Governance versus management process. ISACA, COBIT 5, 2012, www.isaca.org/cobit

Fig. 2.15 Role of IT in the organization. Adapted from: Nolan R., McFarlan F.W., IT Governance and The Board, Harvard Business Review, 2005



to identify appropriate governance structures and processes that enable that strategic choice. As an example, it would be an appropriate choice, in terms of governance structures, to have the CIO report to the CEO or be a member of the Executive Committee in this context (Fig. 2.15).

Based on the governance activities at board-level, business and IT management plans, builds, runs, and monitors activities (an interpretation of Deming's PDCA circle Plan, Do, Check, Act) in alignment with the direction set by the governance body to achieve the enterprise objectives (ISACA, 2012). This all is in line with the definition as formulated in the beginning of this chapter: IT governance is the board's accountability/responsibility and the execution is executive's accountability/responsibility.

In their 2014 study, Turel and Bart (2014) concluded that “High levels of board-level ITG, regardless of existing IT needs, increased organizational performance.” The importance of board involvement is clearly demonstrated in this paper. However, other studies also point out that on average the involvement of boards in enterprise governance of IT is low and that boards should become more IT savvy to be able to govern the digitized organization. Andriole published an article in this context in 2009 and titled his work “The Surprising State of Practice,” which reported on the “surprising” low maturity of boards in this area.

A related research area concerns how boards report on IT governance towards the market and their investors. Drawing on voluntary disclosure theory and the notion of information asymmetry, research in IT governance has clearly advocated the importance of IT governance communications to external stakeholders of the firm (Gordon et al. 2010; Raghupathi, 2007). The theoretical underpinning, rooted in voluntary disclosure theory and agency theory predicts that firms can improve their liquidity and firm valuation through better information intermediation, enhance market reputation, reduce litigation costs, and the cost of capital (Healy and Palepu, 2001). Building on this theoretical premise of an association between potential economic benefits and voluntary disclosure, our research (Bünten et al., 2014) posited and demonstrated that a higher maturity of IT governance activities enables boards to create a better IT information environment and dissemination capability.

In order to assess the level of IT governance disclosure, we used the IT Governance Disclosure Framework developed by Joshi et al. (2013). This framework consists of 39 disclosure items across four broad ITG domains, namely IT

strategic alignment (ITSA), IT value delivery (ITVD), IT risk management (ITRM), and IT performance management (ITPM). ITSA is concerned with the linkage of strategy, architecture, and processes on the IT and business side (Henderson et al., 1993), whereas ITVD is related to “providing IT products and services on time, within budget, and with appropriate quality” (Joshi et al., 2013). ITRM investigates various IT risks such as operational, business continuity and security risk, while ITPM focuses on IT expenses and budgets. Each domain contains several items, indicating the existence of ITG-related features within that domain. Using this ITG disclosure framework, we recorded the data on IT governance reported in the annual reports of the sample firms (Fig. 2.16).

Against this framework, also the annual reports of 2012 of 21 Belgian en Dutch listed companies were analyzed (Caluwe, 2014). The results show that the category which is most reported on is IT risk management. An explanation can be provided by the Belgian and Dutch corporate governance codes. These state that organizations need to report on systems for risk and internal control. Since IT keeps growing in importance in today’s organizations, IT risk is often included. Topics from the category IT performance measurement are also mentioned relatively often. However, this can be attributed to two topics within this category. All companies in the sample report on the topic “IT-related assets are mentioned under intangible assets” and 67 % mention the IT software cost. Again, regulation can provide an explanation. Listed companies are required to make up their financial statements in accordance with the International Accounting Standards (IAS). According to IAS 38, software is a part of the intangible assets. The topics that belong to the category IT value delivery are mentioned fairly often as well. “IT is explicitly mentioned for achieving specific business objectives” is included in 90 % of all analyzed annual reports. Indeed, investors attach importance to the value creation from IT investments. Lastly, companies report very little on IT strategic alignment. Seven out of 11 topics are not included in any of the annual reports. Within this category, topics relating to IT governance at the level of the board of directors were included. According to the interviews and literature, boards of directors pay little attention to IT governance due to a lack of IT expertise among their members.

Assignment Box 2.5: Understanding the Difference Between Governance and Management of IT

Considering this section on Enterprise Governance of IT and the Board, distinguish between governance and management practices in the KLM case.

ITG disclosure framework (adapted from Joshi et al., 2013)	
Domain	Item ID/Description
IT Strategic Alignment (ITSA)	ITSA1 IT expert on board
	ITSA2 IT expert with experience on board
	ITSA3 CIO or equivalent position in firm
	ITSA4 IT committee
	ITSA5 IT risk part of audit/risk committee
	ITSA6 IT is part of audit committee
	ITSA7 IT steering committee
	ITSA8 IT planning committee
	ITSA9 Technology committee
	ITSA10 IT committee at executive level
	ITSA11 CIO or equivalent on board
IT Value Delivery (ITVD)	ITVD1 ITG governance framework/standard
	ITVD2 IT issue in board meeting
	ITVD3 Advise on IT by board
	ITVD4 Section on IT project in annual report
	ITVD5 IT mentioned as strategic business issue
	ITVD6 IT projected as strength
	ITVD7 IT projected as opportunity
	ITVD8 Project update or comments
	ITVD9 IT explicitly mentioned for achieving business objectives
	ITVD10 Comments/Updates on IT performance
	ITVD11 IT training
	ITVD12 Green IT
	ITVD13 In/Outsourcing of IT
IT Risk Management (ITRM)	ITRM1 IT referred to under operational risk
	ITRM2 Special IT risk management program
	ITRM3 Use of IT for regulation & compliance
	ITRM4 Electronic Data Processing
	ITRM5 IT security policy/plan
	ITRM6 IT support for accounting
	ITRM7 Business continuity plan
IT Performance Management (ITPM)	ITPM1 Explicit information on IT expenditure
	ITPM2 IT budget
	ITPM3 IT hardware costs
	ITPM4 IT software costs
	ITPM5 Explicit IT manpower cost
	ITPM6 IT expenses mentioned under administrative cost
	ITPM7 IT related assets mentioned under intangible assets
	ITPM8 Direct cost on IT mentioned in percentage

Fig. 2.16 Enterprise governance of IT disclosure framework. Joshi, A., Bollen, L., & Hassink, H. (2013). An empirical assessment of IT governance transparency: Evidence from commercial banking. *Information Systems Management*, 30(2), 116-136

2.5 Interorganizational Governance of IT

While there is substantial research available on intraorganizational governance of IT, there is a lack of research that specifically looks at how organizations define their interorganizational governance of IT (Croteau and Bergeron, 2009; Grant and Tan, 2010; Croteau and Dubsky, 2011). Many organizations are however operating more and more in complex networked systems, often facilitated by innovations through IT (e.g., e-business), and many industries are using “network governance”—rather than bureaucratic structures within firms—to underpin their value chain (Jones et al., 1997; Chi and Hollsapple, 2005).

Jones et al. (1997) define network governance as “a select, persistent, and structured set of autonomous firms (as well as non-profit agencies) engaged in creating products or services based on implicit and open-ended contracts to adapt to environment contingencies and to coordinate and safeguard exchanges” (p. 914). This network governance perspective clearly poses new challenges for the governance of IT (Croteau and Bergeron, 2009). “These challenges revolve around the allocation of accountability, responsibility and decision rights in network arrangements where there is distributed ownership of ICT resources, systems and processes” (Grant and Tan, 2010).

According to Croteau and Bergeron (Croteau and Bergeron, 2009), this need for interorganizational governance of IT “is also observed within large organizations with several business units where each of them has its own mission, strategy, structure, processes and IT infrastructure and architecture. The challenge for such organizations is to create an inter-unit governance of IT that is developed in a similar way to the interorganizational governance of IT.” These authors define interorganizational governance of IT as the authority and accountability frameworks put in place to encourage the efficient and effective use of IT when sustaining electronic exchanges among business partners, which is dependent on a mix of structures, processes, and participants (relational mechanisms).

As such, it is felt that many of the principles, structures, processes, and relational mechanisms as discussed in KLM case study section (see Sect. 2.3) are of value for any IT governance setup, both intra- as well as interorganizational. Some specific recommendations out of this case towards the interorganizational context are:

An approach towards sourcing decisions in a global economy: Many organizations move towards networked arrangements to (out)source commoditized IT resources. KLM also operates in such a networked environment and developed selective sourcing criteria regarding choosing between allocating work in-house for customized development, or through external IT providers for standardized solutions. Based on the internal “Stay on the Surfboard Principle,” generic business processes that bring no competitive advantage are supported by generic (low development cost, off-the-shelf) applications packages, and business processes, which have the potential to create competitive advantage can and will be supported by in-house custom-built applications. In a networked and global environment, this principle can help in the discussions on what and what not to outsource towards other partners in a networked environment.

An innovative process to allocate resources across multiple business units: KLM is a multi-business-unit environment with distributed ownership over IT resources, systems, and processes. As such, these business units operate in a very similar environment as a network of organizations with shared IT resources. An important challenge for such an environment is to find a way to allocate IT (investment) budgets to business units and/or organizations in line with their specific strategies. KLM uses an innovative and inclusive process to capture and prioritize the, often diverse, business drivers of different business units. The design of this process can be inspirational for other multi-unit or interorganizational environments, as a way to engage—sometimes diverse—business units in the decision-making process around shared IT resources.

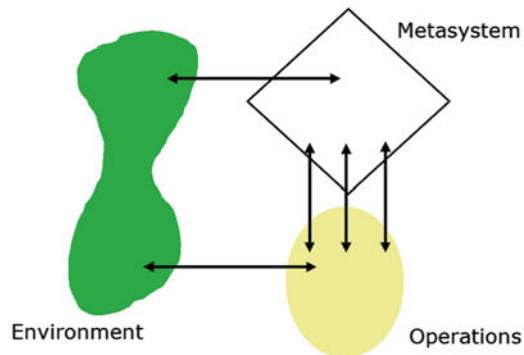
The need for an overarching function: When building a governance model for an inter-organizational or multi-business unit environment, the focus should be on the optimal value creation of the network (of organizations or units) as a whole. At KLM, the individual business units drive the current portfolio management processes and there is no real aggregation at KLM corporate level. However, The executive committee plays a crucial role in the optimization at group level, they are responsible for ensuring that the bottom-up portfolio management process in the end leads to optimal value creation of the KLM group (of business units) as whole. The existence of such overarching function, taking accountability for the governance of IT, appears to be crucial is guarding the value creation of the network (or organizations and units) as a whole.

An approach to manage multi-unit infrastructure investments: It is often difficult to build a business case for infrastructure investment because benefits are typically hard to articulate and spread across multiple units or organizations. At KLM, the CIO-Office manages a specific budget oriented towards these type of cross-unit (cross-organization) infrastructure investments. The CIO-office builds business cases that can apply for this budget, which are derived from the emerging business cases of the business units (to understand future infrastructure needs). This approach ensures that future infrastructure investments will be done required to support the network of business units (or organizations). To build a solid infrastructure in a networked environment, such role of a CIO-Office managing the future infrastructure needs and investments, can be a powerful mechanism.

2.6 Theoretical View on EGIT: Viable Systems Theory

The extant research often shows us descriptively how organizations are implementing IT governance, which IT-related decisions are governed and how they are governed. However, there is little focus on understanding in a more theoretical way what functions are required in an IT governance model and why. We suggest that the Viable Systems Model (VSM) can provide an unexplored perspective and help in focusing on functions that are required for achieving homeostasis in a complex adaptive system and in building a theory of governance of IT Peppard, (2005). Moreover, it takes a more comprehensive perspective of alignment, including

Fig. 2.17 Basic structure of the viable systems model



addressing the execution of projects and programmes that emerge from the alignment process, in the delivery of any expected value.

The VSM was developed in the 1950s by Beer, who first applied its principles to the steel and publishing industries. It was originally derived from his thinking about the “management” of the muscles by the brain and nervous systems, which he then applied to organizations. Beer wrote that a viable system is one that is able to maintain a separate existence and any system “that is capable to maintain its identity independently of other such organisms within a shared environment” (1979, pp. 21–22). In addition to variety, the notion of recursion is a fundamental concept of the VSM. For Beer, “any viable system contains, and is contained in, a viable system” (1979, p. 118). This means that every system contains subsystems that are able to maintain a separate existence, and that each of those viable subsystems has the same fundamental structure as the meta-system.

Like any model, the VSM is a generalized model that can be used to describe any organization. Proponents of the VSM claim that all self-organizing systems conform to this model, even if participants are unaware of this. The VSM treats an organization as an information processing system as it strives to maintain balance. It provides a framework for diagnosing the structure of an organization, its ability to communicate internally and externally, and its effectiveness in controlling the deployment of its resources. A VSM always relates to a purpose; a multipurpose system requires the construction of several VSMs. According to the VSM logic, self-organizing systems have

- Elements which do things (operations)
- Elements which control the doer (management or meta-system)
- Surroundings in which they function (the environment)

While the basic structure shown in Fig. 2.17 illustrates how VSM is typically drawn, in reality the environment should go all the way around both the operation and its meta-system, and the meta-system should be embedded in the operations; for clarity, they are shown separately.

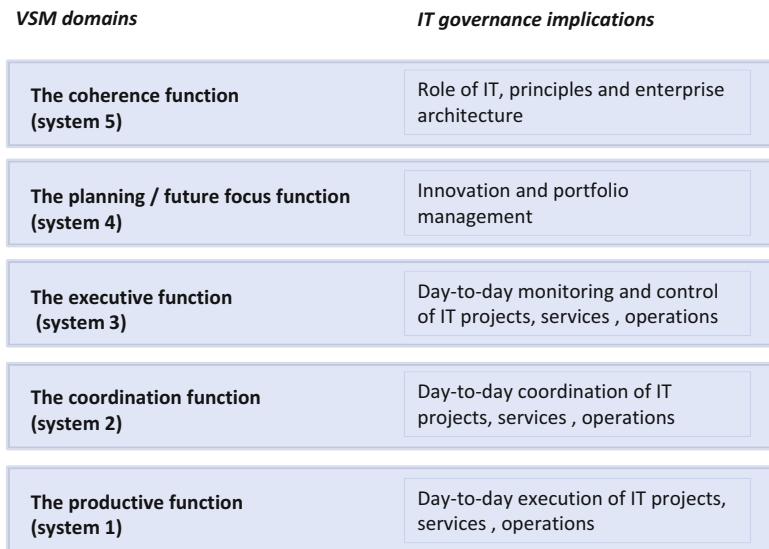


Fig. 2.18 A VSM for IT governance

The VSM has five subsystems, or functions, each having a specific task for maintaining the stability of the system. The VSM identifies these five functions as systems one through five. They are, respectively, the productive function, the coordination function, the executive function, the planning and future focus function, and the coherence function (see Fig. 2.18). All that goes on in an organization can be described in terms of one or more of these functions.

2.6.1 *System 1: The Productive Function*

The System 1 (S1) activities are the operations or wealth-producing parts of the enterprise. They carry out the tasks that the system is intended to accomplish (i.e., implementation of the system's purpose). All other VSM subsystems are management—or decision-making—rather than action oriented.

2.6.2 *System 2: The Coordination Function*

System 2 (S2) is the coordination function, sometimes referred to as the “anti-oscillation function” because it keeps the different activities of the operations running smoothly and keeps them from stepping on each other’s heels. Beer (1979) provides the example of a school timetable; it is a service that ensures that a teacher has only one lecture at any one time period and that only one class uses a room at a given lesson slot.

2.6.3 System 3: The Executive Function

System 3 (S3) is the executive function, where day-to-day management responsibility lies (i.e., resource allocation, control, and monitoring of S1). It oversees the productive operations and manages their common resources, staff, capital, and budgets to secure efficiency of operations. Importantly, it does not determine strategy, define principles, or make policies but interprets these for the S1 activities. While Beer's original model also had a System 3*, ("three star" on the language of the VSM) we have subsumed these functions into System 3. In light of the agreed purpose, and based on the information regarding the state of System 1, Systems 3 influences System 1 by direct intervention or by modification of System 2. Moreover, it audits activities to sustain accountability and internal homeostasis.

2.6.4 System 4: The Planning and Future Focus Function

System 4 (S4), the planning and future focus function, like System 1, is connected directly to the environment. It includes research and development, market research, new products, and strategic planning. It investigates new technologies and customer needs. It emphasizes learning not only about the environment but also what is and isn't working in the organization. In many ways, it is akin to Simon's (1960) notion of intelligence as scanning the environment, both internal and external, seeking to identify problems and opportunities.

2.6.5 System 5: The Coherence Function

System 5 (S5) is the coherence function, maintaining the organizational identity and balancing the organization's present and future requirements. It considers the organization's purpose or identity and is thus responsible for the direction of the whole system. Considering the information generated by S4, it creates policies that are conveyed to S3 for implementation by S1. S5's second task is to monitor the balance between the long-term actions suggested by S4 and the short-term requirements articulated by S3. "System 5 must ensure that the organization adapts to the external environment while maintaining an appropriate degree of internal stability" (Jackson, 1991, p. 111).

2.7 Applying the VSM in the Context of Enterprise Governance of IT

The objectives of the VSM have strong resonance with those of IT governance: To provide stability and coherence and optimize performance. Furthermore, the language of the VSM also reflects the language found in the discourse on IT

governance; words such as adaptation, control, monitoring, coordination, synergy, balance, and policy, are prominent within this literature. Given its heritage, focus, and application, we suggest that the VSM can help in progressing both understanding and practice in relation to IT governance as well as theory development.

The VSM model can be used to assess the objectives of an existing IT governance structure and associated mechanisms and processes. To facilitate such analyses, it was felt that Beer's terminology should change towards more evocative and relevant language in the context of the contemporary discourse. The labels assigned to some of the systems are somewhat dated and have been superseded by a newer and more relevant nomenclature. For example, "policy" had specific meaning in the 1960s—as in business policy—and is today more appropriately referred to as strategy. In the IT and computing literature, policy also has a precise meaning, referring to a guideline, standard, rule, or prescription.

The new proposed terms for the VSM are as follows: Day-to-day execution of IT projects, IT operations, and service delivery (System 1); day-to-day coordination of IT projects, IT operations, and service delivery (System 2); day-to-day monitoring and control (including resource allocation and synergies) of IT projects, IT operations, and service delivery; innovation and portfolio management (System 4); and role of IT, governance principles, and architecture (System 5).

The VSM defines the functions (i.e., coordination, resource allocation, etc.) necessary for an entity to self-organize. It also recognizes that in self-organizing, the entity is not immune to what is happening in the external environment (i.e., new technologies, competitor moves, etc.). Working from the VSM model for IT governance as described above, it is possible to move on to assess how the organization handles the objectives and requirements of each of the functions.

Assignment Box 2.6 Viable Systems Model and IT Governance

Revisit the KLM case discussed in this chapter. Analyze the identified EGIT practices and categorize them according to the five VSM areas as discussed above (see template). Be prepared to justify your categorization and discuss where there are areas for improvement identified using VSM as a lens.

VSM domains	IT governance implications	IT governance practices (processes, structures, relational mechanisms)
The coherence function (system 5)	Role of IT, principles and enterprise architecture	→ []
The planning / future focus function (system 4)	Innovation and portfolio management	→ []
The executive function (system 3)	Day-to-day monitoring and control of IT projects, services , operations	→ []
The coordination function (system 2)	Day-to-day coordination of IT projects, services , operations	→ []
The productive function (system 1)	Day-to-day execution of IT projects, services , operations	→ []

Summary

Having developed a high-level model for Enterprise Governance of IT does not imply that governance is actually working in the organization. Conceiving the model for Enterprise Governance of IT is the first step, deploying it throughout all levels of the organization is the next challenging step. To achieve this, Enterprise Governance of IT can be deployed using a mixture of various structures, processes, and relational mechanisms. These practices need to be embedded at both the level of the board as executive and senior management in the organization.

It is important to recognize that each of the applied processes, structures, and relational mechanisms serve specific or multiple goals in the complex alignment challenge. This chapter discussed the VSM as a lens to better understand these different layers of objectives in enterprise governance of IT.

However, dividing the Enterprise Governance of IT framework into smaller pieces, and solving each problem separately, does not always solve the complete problem. A holistic approach towards Enterprise Governance of IT acknowledges its complex and dynamic nature, consisting of a set of interdependent subsystems (processes, structures, and relational mechanisms) that deliver a powerful whole. The challenge for organizations is to select an appropriate set of practices, specifically for their own environment. To assist organizations in this challenge, this chapter discussed a list of Enterprise Governance of IT practices and illustrations of their application in the context of the airline company KLM.

Study Questions

1. Discuss and illustrate important structures for Enterprise Governance of IT.
2. Discuss and illustrate important processes for Enterprise Governance of IT.
3. Discuss and illustrate important relational mechanisms for Enterprise Governance of IT.
4. Explain the difference between enterprise governance and enterprise management of IT.
5. Identify and discuss governance practices that are most relevant for obtaining board involvement.
6. Discuss how the VSM is related to Enterprise Governance of IT and how it can be used to analyze EGIT implementations.
7. Discuss why boards should report on IT governance and what they could report about in this context.

Acknowledgments We would like to express our special gratitude towards Prof. Dr. Joe Peppard who worked with us on developing a more theoretical view on Enterprise Governance of IT. Special thanks also to John Thorp and Dirk Gemke for their very inspiring thoughts and contributions in the development of the KLM case on enterprise governance of IT. Finally, special appreciation for the joint effort with Dr. Joshi Anant on understanding IT governance transparency.

References

- Andriole, S. (2009). Boards of directors and information technology governance: The surprising state of practice. *Communications of the AIS*, 24(22), 373–394.
- Beer, S. (1979). *The heart of the enterprise*. Chichester, England: Wiley.
- Bünten, S., Joshi, A., De Haes, S., & Van Grembergen, W. (2014). Understanding the association between IT governance maturity and IT governance disclosure. *International Journal on IT/Business Alignment and Governance*, 5(1), 16–33.
- Caluwe, L. (2014). *IT governance transparency*. Master thesis project submitted for achieving the degree of business engineer in information systems management, supervised by Prof. Dr. Steven De Haes, Faculty of Applied Economics, University of Antwerp.
- Chi, L., & Hollsapple, C. (2005). Understanding computer-mediated interorganizational collaboration: A model and framework. *Journal of Knowledge Management*, 9(1), 53–75.
- Croteau, A.-M., Bergeron, F. (2009). Interorganizational governance of information technology. In *Proceedings of the 42nd Hawaii International Conference on System Sciences, Big Island, HI*.
- Croteau, A.-M., Dubsky, J. (2011). Uncovering modes of interorganizational governance of IT. In *Proceedings of the 44th Hawaii International Conference on System Sciences, Kauai, HI*.
- De Haes, S., Dirk, G., John, T., & Van Grembergen, W. (2011). KLM's enterprise governance of IT journey: From managing IT costs to managing business value. *MISQ Executive*, 10(3), 109–120.
- 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.
- Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 34(3), 567–594.
- Grant, T. G., Tan, F. (2010). Call for papers European Journal of Information Systems: Special issue on governing IT in inter-organizational relationships. Retrieved October 12, 2010, from <http://www.palgrave-journals.com/ejis/index.htm>.
- Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics*, 31, 405–440.
- Henderson, J. C., Venkatraman, N., & Oldach, S. (1993). Continuous strategic alignment: Exploiting information technology capabilities for competitive success. *European Management Journal*, 11(2), 139–149.
- ISACA. (2012). COBIT 5. Retrieved from www.isaca.org.
- Jones, C., Hesterly, W., & Borgatti, S. (1997). A general theory of network governance: Exchange conditions and social mechanisms. *Academy of Management*, 22(4), 911–645.
- Joshi, A., Bollen, L., & Hassink, H. (2013). An empirical assessment of IT governance transparency: Evidence from commercial banking. *Information Systems Management*, 30(2), 116–136.
- Nolan, R., & McFarlan, F. W. (2005). Information technology and the board of directors. *Harvard Business Review*, 83(10), 96–106.
- Peppard, J. (2005) The application of the viable systems model to information technology governance', in *Proceeding of the International Conference of Information Systems (ICIS)*.
- Raghupathi, W. R. P. (2007). Corporate governance of IT: A framework for development. *Communications of the ACM*, 50(8), 94–99.
- Turel, O., & Bart, C. (2014). Board-level IT governance and organizational performance. *European Journal of Information Systems*, 23, 223–239.
- Van Grembergen, W. (Ed.). (2004). *Strategies for information technology governance*. Hershey, PA: Idea Group.

Chapter 3

Business/IT Alignment

Abstract Previous chapters described what Enterprise Governance of IT is about and how a set of practices can be leveraged to implement Enterprise Governance of IT. In this chapter, the impact of Enterprise Governance of IT implementations on business/IT alignment will be discussed. The first question is how an organization can measure and evaluate its current status of business/IT alignment. This discussion has supplemented a study that illustrates the relationship between Enterprise Governance of IT and alignment, and an exploration of the impact of cultural issues on alignment maturity.

3.1 Measuring Business/IT Alignment

The concept of business/IT alignment was already defined in Chap. 1. This chapter explained that business/IT alignment is about aligning business strategy, IT strategy, business operations, and IT operations and as such, it was concluded that alignment is a complex challenge for organizations.

There is no universal way to measure business/IT alignment described in literature. Many researchers have developed models that attempt to capture the complex alignment construct as complete as possible. Each measurement model has its own approach, and as a result, it is very difficult to compare results of alignment studies. Some potential approaches are discussed below, all having their strengths and weaknesses. In the end, it is important to select the approach that is most suited for the type of activity or research one is trying to do.

3.1.1 *The Matching and Moderation Approach*

The matching approach looks at the difference in rating between two pairs of related items. When there is a high difference between the ratings of related items, alignment is low, and oppositely, when there is a low difference, alignment is high. Figure 3.1 illustrates the matching approach.

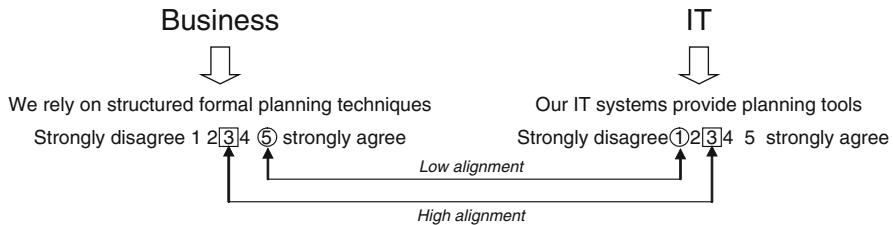


Fig. 3.1 Matching approach

In this type of studies, researchers look for parallelism between business and IT. If the difference in scores between business and IT is high, alignment is low (in Fig. 3.1, difference in scores for low alignment is 5), and oppositely, if the difference between the scores is low, alignment is high (in Fig. 3.1, difference in scores of high alignment is 0). Applying this for a set of questions can lead to an alignment score for the organization. One of the shortcomings of this method is the question whether the scores necessarily need to be at the same level to indicate high degrees of alignment. Take the example in Fig. 3.1: it is clear that if the business scores 5 on formal planning techniques and IT scores 1 on providing planning tools that alignment is low as IT is not supporting business needs. However, if the business does not rely on structured formal planning techniques (score 1 on left hand side) but IT scores a better rate of 2 or 3 on providing planning tools, IT maybe outperforming slightly but does that really imply low alignment? However, this method is clearly an intuitive and simple approach to undertake and therefore often used in practice and research.

A related technique is the moderation approach. In this approach, alignment is viewed as an interaction rather than a parallelism, and in this way quite different in outcomes compared to the moderation approach. It is the combination or synergy between business and IT, rather than the difference, which is important. The moderation approach does not calculate the difference but the product terms. In the example of Fig. 3.1, this implies that the business score of 1 and the IT score of 5 result in an alignment score of 5 and the business score of 3 and the alignment score of 3 in 9. It is clear that this approach differs from the matching approach as two low scores are now seen as “low alignment” where in the matching approach, two (equal) low scores result in “high alignment.” The basic assumption in the moderation approach is that the interactive relationship (moderation) between business and IT, and not the difference, will impact business performance. For example, two 3’s would lead to an alignment score of 9 and two 5’s would lead to an alignment score of 25 following the moderation approach. In the matching approach, both scenarios would lead to an alignment score of “0”, i.e., high alignment. In the moderation approach, the higher score of 25 (two 5’s) is assigned as this represents a higher interaction effect between business and IT which will impact firm importance.

Whatever method is chosen, matching or moderations, it should be clear that both approaches are valuable but that they can lead to different conclusions regarding business/IT alignment in an organization.

3.1.2 *The Profile Deviation Approach*

Measuring alignment based on the profile deviation approach is based on two steps. First, an “ideal alignment scenario” has to be deducted (from theory) and next, deviations from this ideal state are calculated.

A well-known example here is the study of Sabherwal and Chan (2001). These authors tried to define IT strategies that map best on specific business strategies. Those business strategies were defined based on the Miles and Snow typology, which identifies different types of business strategies: defenders (aiming to reduce costs, maximizing efficiency and effectiveness of production, avoiding organizational change), prospectors (seen as leading innovators, reacting first on signals of change in their market), and analyzers (closely watching competitor’s activities and carefully evaluating organizational changes). Figure 3.2 demonstrates which IT strategies align best with specific business strategies, according to their insights. “IT for efficiency” is oriented towards internal and interorganizational efficiencies and long-term decision making and maps well on the defender’s business strategy. “IT for flexibility” focuses on market flexibility and quick strategic decisions which maps on the prospector’s business strategy. “IT for comprehensiveness” enables comprehensive decisions and quick responses through knowledge of other organizations which complies with the analyzer’s business strategy.

Based on this model, organizations can be classified against each of the categories and the distance against the ideal state can be calculated. It is clear that the value of this type of measurement stands or falls with the validity of the theorized ideal state model.

3.1.3 *The Scoring Approach*

A typical example of the scoring approach is the information economics method developed by Parker et al. (1988). This scoring method can be used as an alignment measurement whereby both business and IT people, score major IT investments to verify the degree of alignment against a set of business and IT criteria. The method typically departs from the Return On Investment (ROI) of a project and different non-tangibles such as “strategic match of the project” (business evaluation) and “match with the strategic IT architecture” (IT evaluation). In essence, information economics is a scoring technique for projects, resulting in a weighted total score

<i>Business Strategy</i>	Defenders	Prospectors	Analyzers
<i>IT Strategy</i>			
IT for efficiency	High	Low	Low
IT for flexibility	Low	High	Low
IT for comprehensiveness	Low	Low	High

Fig. 3.2 Mapping IT and business strategies. Based on: Sabherwal, R., & Chan, Y. (2001). Alignment between business and IS strategies: a study of prospectors, analyzers and defenders. *Information Systems Research*, 12(1), 11–33

based on the scores for the ROI and the non-tangibles. Typically scores from 0 to 5 are attributed whereby 0 means no contribution and 5 refers to a high contribution; the values obtain a positive score and the risks a negative score (Fig. 3.3).

A limitation of previous approach is clearly that it is focused only on one major IT project. Alternative scoring instruments are developed by Weill and Broadbent (1998) and Weill and Ross (2004). These researchers developed a “diagnostic to assess alignment” and “governance performance indicator” as visualized in Figs. 3.4 and 3.5. This first diagnostic requires the respondents to assess ten

<i>Traditional ROI (+)</i>		
+ value linking (+) + value restructuring (+) + value acceleration (+) + innovation (+)		
= Adjusted ROI	+ Business Value	+ IT Value
	<ul style="list-style-type: none"> ■ Strategic match (+) ■ Competitive advantage (+) ■ Competitive response (+) ■ Management information (+) ■ Service and quality (+) ■ Environmental quality (+) ■ Empowerment (+) ■ Cycle time (+) ■ Mass customization (+) 	<ul style="list-style-type: none"> ■ Strategic IT architecture (+)
	- Business Risk	- IT Risk
	<ul style="list-style-type: none"> ■ Business strategy risk (-) ■ Business organization risk (-) 	<ul style="list-style-type: none"> ■ IT Strategy risk (-) ■ Definitional uncertainty (-) ■ Technical risk (-) ■ IT service delivery risk (-)
= VALUE (business contribution)		

Fig. 3.3 Information Economics. Based on: VAN GREMBERGEN W. AND VAN BRUGGEN R., 1997, *Measuring and improving corporate Information Technology through the balanced scorecard technique*, In proceedings of the European Conference on the Evaluation of Information Technology, Delft, The Netherlands

	always true				never true
1. Senior management has no vision for the role of IT	1	2	3	4	5
2. The IT group drives IT projects	1	2	3	4	5
3. There is no IT component in the division's strategy	1	2	3	4	5
4. Vital information necessary to make decisions is often missing	1	2	3	4	5
5. Islands of automation exist	1	2	3	4	5
6. Management perceives little value from computing	1	2	3	4	5
7. A "them and us" mentality prevails	1	2	3	4	5
8. IT doesn't help for the hard tasks	1	2	3	4	5
9. It's hard to get financial approval for IT projects	1	2	3	4	5
10. Senior management sees outsourcing as a way to control IT	1	2	3	4	5
Average:					

Fig. 3.4 Diagnostic to assess alignment. Adapted from: Weill P. and Broadbent M., Leveraging the new Infrastructure: how market leaders capitalize on information technology, Harvard Business School Press, 1998

1. How important are the following outcomes of your IT governance, on a scale from 1 (not important) to 5 (very important)?					
	Not important				Very important
	1	2	3	4	5
Cost-effective use of IT					
Effective use of IT for growth					
Effective use of IT for asset utilisation					
Effective use of IT for business flexibility					
2. What is the influence of the IT governance in your business on the following measures of success, on a scale from 1 (not important) to 5 (very important)?					
	Not important				Very important
	1	2	3	4	5
Cost-effective use of IT					
Effective use of IT for growth					
Effective use of IT for asset utilisation					
Effective use of IT for business flexibility					

Fig. 3.5 Governance outcome survey. Adapted from: Weill P. and Ross J., IT Governance: how top performers manage IT decisions rights for superior results, Harvard Business School Press, 2004, 269 blz

$$\frac{(\sum_{n=1}^4 (\text{importance of outcome } \{Q1\} * \text{influence of IT governance } \{Q2\})) * 100}{\sum_{n=1}^4 (5 * (\text{importance of outcome}))}$$

Fig. 3.6 Governance performance calculator. Adapted from: Weill P. and Ross J., IT Governance: how top performers manage IT decisions rights for superior results, Harvard Business School Press, 2004, 269 blz

statements that relate to the degree of alignment, on a scale from 1 to 5 (1 = always true, 5 = never true). The average of the assessments on all the ten statements provides the alignment score.

The governance performance measure is based on the scores regarding perceived governance outcome, i.e., strategic alignment. Respondents have to score on a scale from 1 (not important) to 5 (very important) on how important a particular governance outcome is (Q1), and how well IT governance contributed to meeting that outcome (Q2) (1 = not successful, 2 = very successful) as visualized in Fig. 3.5. The outcomes that are to be scored are cost-effective use of IT, effective use of IT for growth, effective use of IT for asset utilization, and effective use of IT for business flexibility. In other words, Q1 assesses the importance of a particular outcome and Q2 assesses how well IT governance contributed to meeting the outcome.

Based on the scores a weighted governance performance can be calculated, using the formula of Fig. 3.6. Since not all firms rank the outcomes with the same

importance, the answers to the first question are used to weight the answers of the second question. Then the weighted scores for the four questions are added and divided by the maximum score attainable by that enterprise.

3.1.4 The Maturity Model Approach

Organizations can also use a maturity model to assess the current degree of alignment. This is a method of scoring that enables the organization to grade itself from nonexistent (0) to optimized (5). This tool offers an easy-to-understand way to determine the “as-is” and the “to-be” (according to enterprise strategy) position and enables the organization to benchmark itself against best practices and standard guidelines. In this way, gaps can be identified and specific actions can be defined to move towards the desired level of strategic alignment maturity.

A good example of strategic alignment maturity models was developed by Luftman (2000). Luftman defines five maturity levels around six alignment-related domains (e.g., communication, partnership), using the criteria and attributes described in the first two columns of Fig. 3.7. The last two columns indicate the characteristics or values of each attribute to obtain a level 1 or level 5 of the maturity model.

Based on this model, Luftman reports on international business/IT alignment benchmarks. One example is given in Fig. 3.8 which shows that retail and transportation sector are leading the benchmark and maybe surprisingly the financial sector that also achieve an average outcome.

Assignment Box 3.1: Business/IT Alignment Benchmarking

Compare the international business/IT alignment results as presented in Fig. 3.8 and try to explain the differences between industries.

3.2 Aligning Business Goals and IT Goals

To provide practitioners with hands-on guidance in the business/IT alignment domain, a research project by the University of Antwerp—Antwerp Management School (Van Grembergen et al. 2007) worked on developing pragmatic insights into how specific enterprise goals can drive IT goals and vice versa, as visualized in Fig. 3.9. If “maintaining the enterprise reputation and leadership” is an important business goal, a supporting IT goal could be “ensuring IT services can resist and recover from attacks.”

<u>attribute</u>	<u>characteristics level 1</u>	<u>characteristic level 5</u>
•communications maturity		
• understanding of business by IT • understanding of IT by business • inter/intra-organizational learning • protocol rigidity • knowledge sharing • liaison(s) breath/effectiveness	minimum minimum casual, ad hoc command and control ad hoc none or ad hoc	pervasive pervasive strong and structured informal extra-enterprise extra-enterprise
• competency/value measurements maturity		
• IT metrics • business metrics • balanced metrics • service level agreements • benchmarking • formal assessments/reviews • continuous improvement	technical ad hoc ad hoc, unlinked sporadically present not generally practiced none none	extended to external partners extended to external partners business, partner and IT metrics extended to external partners routinely performed with partners routinely performed routinely performed
• governance maturity		
• business strategic planning • IT strategic planning • reporting/organization structure • budgetary/control • IT investment management • steering committee(s) • prioritization process	ad hoc ad hoc CIO reports to CFO central/decentral cost center, erratic cost based, erratic not formal, regular reactive	integrated across & external integrated across & external CIO reports to CEO federated investment center, profit center business value partnership value added partner
<u>attribute</u>	<u>characteristics level 1</u>	<u>characteristic level 5</u>
•partnership maturity		
• business perception of IT value • role of IT in strategic business planning • shared goals, risk, rewards/penalties • IT program management • relationship/trust style • business sponsor/champion	IT perceived as a cost no seat at business table IT takes risk ad hoc conflict/minimum none	IT co-adapts with business co-adaptive with business risks and rewards shared continuous improvement valued partnership at the CEO level
•scope & architecture maturity		
• traditional, enabler driver • standards articulation • architectural integration: • functional organization • enterprise • inter-enterprise • architectural transparency, flexibility	traditional systems none or ad hoc no formal integration none	business strategy driver/enabler inter-enterprise standards evolve with partners integrated standard enterprise architecture with all partners across the infrastructure
•skills maturity		
• innovation, entrepreneurship • locus of power • management style • change readiness • career crossover • education, cross-training • attract & retain best talent	discouraged in the business command and control resistant to change none none no program	the norm all executives, including CIO relationship based high, focused across the enterprise across the enterprise effective program for hiring & retaining

Fig. 3.7 The strategic alignment maturity levels of Luftman. Adapted from: Luftman, J., 2000, *Assessing Business-IT alignment Maturity*, Communications of AIS, vol. 4

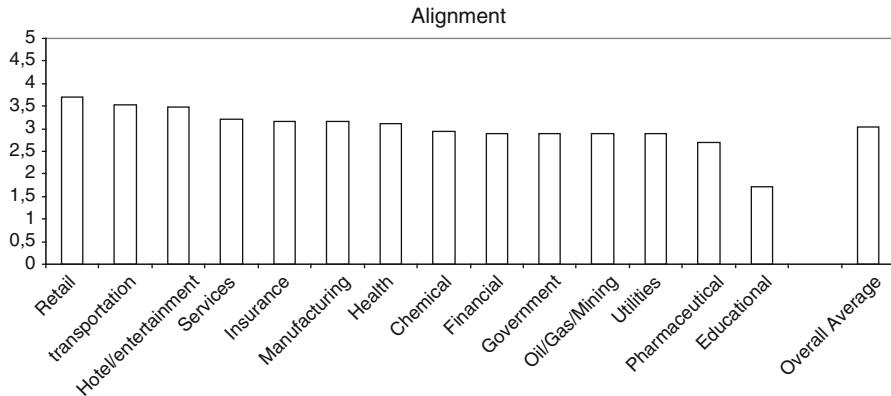


Fig. 3.8 Worldwide Business/IT alignment benchmark. Based on: Luftman J., Kempaiah R., 2007, An Update on Business/IT Alignment: a line has been drawn. MISQ Executive, vol. 6, no. 3

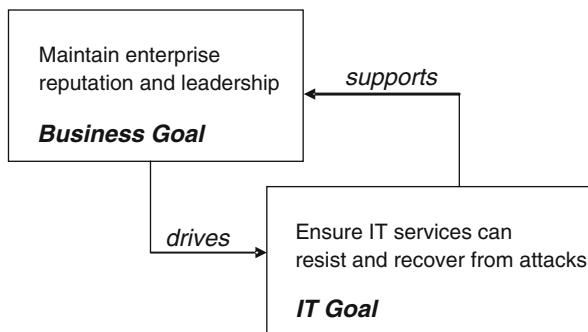


Fig. 3.9 Enterprise goals and IT goals

In order to populate the above model with realistic examples of enterprise goals and IT-related goals, many in-depth interviews with CEO and CIO in different sectors were done and supplemented with expert assessments. A generic list of enterprise goals, IT-related goals, and its inter-relationship was established, as shown in Fig. 3.10. This cascade now constitutes the core entry point for COBIT 5 (see Chap. 5). This model suggests that organizations should always start with analyzing their business/IT strategic alignment through defining and linking enterprise goals and IT-related goals.

Fig. 3.10 Enterprise goals and IT-related goals—2

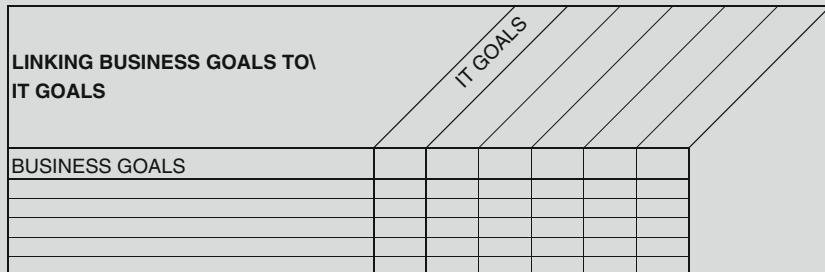
Assignment Box 3.2: Defining and Linking Business Goals and IT Goals

Work in groups of three to five people and choose a specific organization or industry sector. Next, run through the following steps.

Assume that you are the Board or Executive Committee of the organization and define five specific business goals.

Put the business goals aside. Assume you are the IT Management Committee of the same organization, and define five specific IT goals.

Put the business goals and IT goals in a matrix and try to find correlations on how IT goals support business goals.



Discuss and present your conclusions to the group.

3.3 The Relationship Between Enterprise Governance of IT and Alignment

As discussed in the first chapter, the ultimate outcome of Enterprise Governance of IT is business/IT alignment. In this section, we illustrate the relationship between Enterprise Governance of IT and business/IT alignment based on the results of extreme case research (De Haes and Van Grembergen 2009). The research project was aimed at exploring the relationship between IT governance implementations and business/IT alignment. This research started with creating a business/IT alignment benchmark for the Belgian financial services sector based on a sample of ten Belgian financial services organizations. In each organization, it was asked that five to ten senior business and IT managers completed a questionnaire measuring business/IT alignment maturity (on a scale from 0 to 5), based on the Luftman model as discussed in previous sections. From the results of this benchmark, four extreme case organizations were selected (two high performers and two low performers in terms of business/IT alignment), in which a workshop was organized to measure the maturity of the IT governance practices applied based on a generic maturity scale from 0 (nonexistent) to 5 (optimized). The data collected allowed for detailed cross-case analysis, looking for causes that could explain why some organizations achieved a higher business/IT alignment score compared to other organizations.

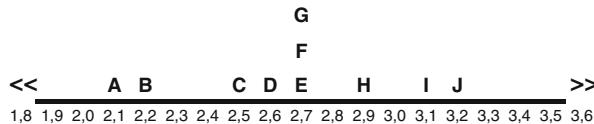


Fig. 3.11 Business/IT alignment maturity benchmark

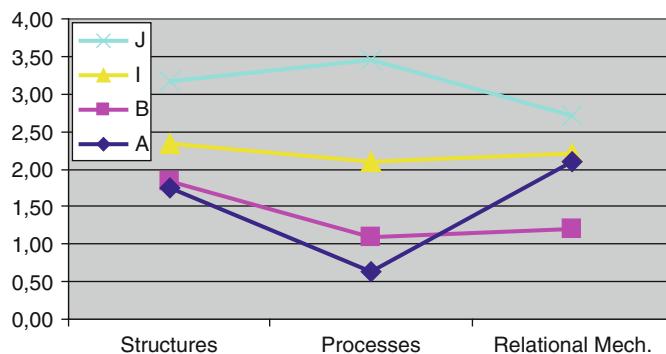


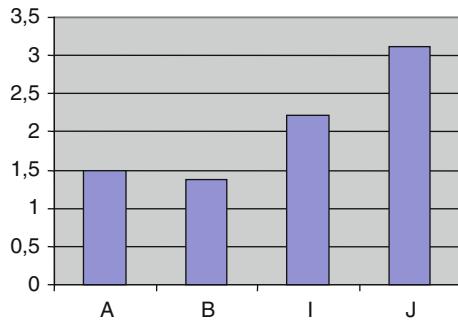
Fig. 3.12 Comparing extreme cases (1)

After measuring alignment in ten Belgian financial services organizations, it appeared that the overall business/IT alignment maturity is 2,69 on a scale of 5 in the Belgian financial services sector (Fig. 3.11).

The benchmark contained two organizations with a relatively high business/IT alignment maturity compared to the overall average (high performers, I–J) and two organizations with a relatively low business/IT alignment maturity compared to the benchmark (low performers, A–B). The other six organizations were all situated around the overall average. An interesting consideration here is what the desired target or to-be situation would be for the financial services sector. There is no literature available in this domain, but taken the high dependency on IT into account, one could argue that at least a maturity level 3 would be required, which implies standardized and documented processes and procedures.

In each of these extreme cases, it was assessed in which maturity (on a scale from 0—nonexistent to 5—optimized) the organization was applying each of the 33 IT governance practices discussed in Chap. 2 (see also Assignment Box 2.2). When comparing the averages of maturity of IT governance practices (structures, processes, and relational mechanisms) in those extreme cases, it appears that in general the high performers have more mature IT governance structures and processes, as shown in Fig. 3.12. This figure also shows that processes on average were less mature compared to structures, indicating that it is more difficult to implement processes compared to structures, which was also discussed in previous section.

Fig. 3.13 Comparing extreme cases (2)



It was also shown that the organizations with low business/alignment maturity did have a lot of practices in place, but the average maturity of these practices was below maturity level 2, as shown in Fig. 3.13. This might indicate that the impact on business/IT alignment of IT governance practices that have a maturity level lower than 2, is limited.

The impact of relational mechanisms on business/IT alignment maturity was not clearly demonstrated in this research. However, a finding was that the two high performers had started their IT governance implementation many years ago and came to a point where many structures and processes were embedded in day-to-day practice. At that time, the importance of relational mechanisms becomes less important. The relational mechanisms are likely very important in the initiating phase of IT governance, in which the two low performers were situated.

An interesting IT governance practice that was not used by any of the organizations, although being promoted by experts and thought leaders as very important (Turel and Bart 2014), is the “IT strategy committee at the level of the board of directors.” This practice is promoted as a structure to ensure that board gets involved in a structured way in IT governance issues. During the interviews, three out of four organizations stated that board involvement in IT governance is not feasible and probably not required. The latter is of course in great contrast with the argumentation of section 2.4 on the role of the board in Enterprise Governance of IT.

3.4 Exploring Culture and Alignment

The central question in this section addresses how national culture influences the alignment of business and IT in organizations. We present a framework for studying national cultures and explore the relationship between culture and alignment (Silvius et al. 2010). The last part of the section presents a small-scale empirical study to explore the expected influence of national culture on alignment maturity.

3.4.1 The Hofstede Framework for Studying National Culture

Hofstede (1991) defines culture as “the collective programming of the mind, which characterizes the members of one organization from others.” By “collective programming” Hofstede refers to the symbols, heroes, rituals, and values that collectively define a culture. Cultures come in many different kinds or layers, such as national cultures, organizational cultures, organizational subcultures, and occupational cultures (Gefen and Straub 1997; Hofstede 1991). This Hofstede framework characterizes culture on the following dimensions.

3.4.1.1 Power Distance Index (PDI)

The power distance index is an indication of the extent to which less powerful members of a society accept unequal distribution of power. It reveals dependence relationships in a country. A low PDI shows limited acceptance of power inequality and less dependence of subordinates on managers. It also shows a preference for consultation and cooperation.

3.4.1.2 Individualism vs. Collectivism (IND)

In cultures that are considered highly individualistic, individuals are loosely tied and are expected to look out for themselves and their family. In “collectivist” cultures, people are integrated into strongly cohesive in-groups, and group loyalty lasts a lifetime. In individualistic cultures, time, punctuality, and schedules are considered highly important, whereas in collectivistic cultures personal relationships and contacts prevail.

3.4.1.3 Masculinity vs. Femininity (MAS)

In the dichotomy masculine versus feminine, a masculine culture values assertiveness, performance, and material success. In a feminine society values like quality of life, tenderness and modesty prevail. In a feminine culture, individuals don’t like to stand out or be unique, whereas in a masculine society success and career are valued highly.

3.4.1.4 Uncertainty Avoidance Index (UAI)

The uncertainty avoidance index is defined as “the extent to which the members of a culture feel threatened by uncertain or unknown situations” (Hofstede 1991). Cultures with a high UAI have a large need for rules and regulations to guide tasks. Cultures with a low UAI are less rule dependent and are more trusting.

Based on follow-up research among students in 23 countries around the world, and criticism that the model represented a very “western” way of thinking, a fifth dimension was added (Hofstede and Bond 1984).

3.4.1.5 Long-Term Orientation vs. Short-Term Orientation (LTO)

This dimension is an indication of the perception of time in a culture and is based on the heritage of Confucius, the most influential Chinese philosopher who lived around 500 BC. Values associated with Long-Term Orientation are thrift and perseverance; values associated with Short-Term Orientation are respect for tradition, fulfilling social obligations, and protecting one’s “face.”

3.4.2 Applying the Hofstede Framework to Explore the Impact of Culture on Business and IT Alignment

(National) Culture influences the way IT is perceived or used. Several authors (Straub et al. 1997; Livonen et al. 1998; Hofstede 2000; Batenburg 2007) found proof of this in their studies. All of these studies show a certain impact of national cultures in the perception and use of IT. Given these findings, it can be expected that culture also influences the alignment of IT and business. This influence however is not reflected in any studies on alignment so far.

In a reaction on his most recent report on the maturity of alignment in organizations (2007), Luftman acknowledges the fact that international companies and international activities are included in the study. The potential influence of national cultures on alignment maturity however is not analyzed in Luftman’s report. Given the impact of national cultures on the use and perception of IT found in earlier studies, it can be expected that cultures could also influence the perception of alignment maturity on the different variables of Luftman’s assessment model (see Fig. 3.14). For example, an expected relationship can be that countries with a higher uncertainty avoidance score place more emphasis on governance of IT, resulting in a higher score on governance maturity and value transparency.

Based on indications provided by literature, the following analysis of the relationship between Hofstede’s dimensions of culture on Luftman’s variables of alignment maturity, can be constructed.

3.4.2.1 Power Distance Index

PDI—Communications maturity: Based on the findings of Sørnes et al. (2004), it can be concluded that a low PDI score indicates close working relationships between hierarchical levels and assertive behavior by subordinates. This can be expected to result in a higher communications maturity because of more intensive and less formalized communication.

<i>BIA maturity variable</i>	<i>Description</i>
Communication	How well does the technical and business staff understand each other? Do they connect easily and frequently? Does the company communicate effectively with consultants, vendors and partners? Does it disseminate organizational learning internally?
Value measurement	How well does the company measure its own performance and the value of its projects? After projects are completed, do they evaluate what went right and what went wrong? Do they improve the internal processes so that the next project will be better?
Governance	Do the projects that are undertaken flow from an understanding of the business strategy? Do they support that strategy? Does the organization have transparency and accountability for outcomes of IT projects.
Partnership	To what extend have business and IT departments forged true partnerships based on mutual trust and sharing risks and rewards?
Scope & Architecture	To what extend has technology evolved to become more than just business support? How has it helped the business to grow, compete and profit?
Skills	Does the staff have the skills needed to be effective? How well does the technical staff understand business drivers and speak the language of the business? How well does the business staff understand relevant technology concepts?

Fig. 3.14 Business/IT alignment (BIA) dimensions of Luftman

PDI—Value measurement maturity: Following the motivation stated under “Communications,” a lower PDI score can be expected to result in less need for creating transparency, procedures, and reports that enhance Value measurement, therefore resulting in a lower maturity on this factor.

PDI—Governance maturity: Again based on the findings of Sørnes et al. (2004) that concluded that a low PDI score indicates close working relationships between hierarchical levels and assertive behavior by subordinates, it should be expected that in cultures with a low PDI there is less need for formalized governance processes, resulting in a relatively lower Governance maturity.

PDI—Partnership maturity: Following the motivation given under “Communications,” a lower PDI score can be expected to result in a higher Partnership maturity because of more intensive, less formalized, and richer communication.

PDI—Scope and Architecture maturity: Given the characteristics of this factor, no indication was found in literature to indicate how the PDI relates to the Scope and Architecture maturity.

PDI—Skills maturity: The high level of assertiveness that is expected to result from a low PDI score is stimulating entrepreneurship and initiative in lower organizational levels and can therefore be expected to result in a high Skills maturity.

3.4.2.2 Individualism vs. Collectivism

IND—Communications maturity: In individualistic societies, the task will normally prevail over personal relationships (Hall 1976; Walls 1993). A high IND score could therefore indicate a much task-oriented communication that will result in a high maturity score, but lacks personal warmth that may be important in case of problems.

IND—Value measurement maturity: Individualistic cultures will normally show a high appreciation of value and performance. It should therefore be expected that these societies score relatively high on Value measurement maturity.

IND—Governance maturity: In Hofstede's study, the United States scores highest (most individualistic) of all nations on this dimension. The United States also developed strongly in governance as a reaction to fraudulent actions of individuals. It should therefore be expected that high IND cultures also score high on Governance maturity.

IND—Partnership maturity: In individualistic cultures, personal task prevails collective tasks (Veiga et al. 2001). A high IND culture should therefore be expected to result in a lower Partnership maturity. On the other hand, van Birgelen et al. (2002) found that in an individualistic culture people therefore seem to be more innovative and trusting in exchange relationships with external parties, which could be reflected in a higher Partnership maturity.

IND—Scope and Architecture maturity: Given the more collective nature of architecture, it can be expected that a high IND culture should reflect in a relatively low score on Architecture maturity. On the other hand, the findings of van Birgelen et al. (2002) mentioned above provide indication that a more individualistic culture reflects in a higher Architecture maturity because of its openness to exchange relationships with external parties.

IND—Skills maturity: A high IND culture can be expected to result in a high Skills maturity because of its appreciation of individual skill development.

3.4.2.3 Masculinity vs. Femininity

MAS—Communications maturity: Hofstede's (2000) findings support the claim that one-way communication will be more prominent in masculine countries, while two-way communication prevails in feminine countries. It should therefore be expected that a high MAS culture scores relatively lower on Communications maturity.

MAS—Value measurement maturity: A high “masculine” culture values value assertiveness and focus on material success, while “feminine” countries value modesty, tenderness, and quality of life (Hofstede 1991). A high MAS score can therefore be expected to score high on Value measurement maturity.

MAS—Governance maturity: Because of its orientation on material success, performance and measurement stated above, a high MAS culture can be expected to score high on Governance maturity.

MAS—Partnership maturity: In more feminine cultures, individuals don't like to stick out, be unique or conspicuous, unlike the more assertive and career-seeking individuals found in masculine cultures (Sørnes et al. 2004). This “live and let live” approach could enhance partnerships between individuals, departments, or organizations. A less MAS culture should therefore be expected to result in a higher Partnership maturity.

MAS—Scope and Architecture maturity: Because of its tendency to appreciate individual performance and success, a more masculine culture should be expected to score lower in Scope and Architecture maturity, which has a nonindividual character.

MAS—Skills maturity: Because of its orientation on work and material success (Hofstede 1991), a high MAS culture should be expected to result in a higher Skills maturity. On the other hand, a more “feminine” culture can be expected to stimulate a more diverse skills development that in fact could also result in a higher Skills maturity score.

3.4.2.4 Uncertainty Avoidance Index

UAI—Communications maturity: A high UAI culture can be expected to score relatively lower on Communications maturity because of its tendency towards certainty which does not stimulate open and informal communication.

UAI—Value measurement maturity: Following the argumentation of Sørnes et al. (2004), a high UAI culture can be expected to avoid uncertainty about value, resulting in a higher score on Value measurement maturity.

UAI—Governance maturity: Following the same argumentation (Sørnes et al. 2004), a high UAI culture can be expected to score high on Governance maturity because of its tendency to require certainty.

UAI—Partnership maturity: Given the fact that “partnership” in general is based more on trust than on certainty, it should be expected that a high UAI culture, scores relatively lower on Partnership maturity.

UAI—Scope and Architecture maturity: A high UAI culture can be expected to score high on Architecture maturity because of its tendency to create certainty and security, and the slower rate of adoption of new technologies found by Png et al. (2001).

UAI—Skills maturity: Based on the findings of Livonen et al. (1998), it can be expected that a high UAI decreases the pace of individual learning and will result in a lower Skills maturity.

	PDI	IND	MAS	UAI
	Power Distance Index	Individualism vs. Collectivism	Masculinity vs. Femininity	Uncertainty Avoidance Index
Maximum score (all nations)	104	91	110	112
Minimum score (all nations)	11	6	5	8
Score for the Netherlands	38	80	14	53
Score for Belgium	65	75	54	94

Fig. 3.15 Belgium and the Netherlands compared Hofstede's variables. *Note:* Because of the fact that Belgium does not have a score on Hofstede's long-term orientation vs. short-term orientation variable, this dimension is discarded

3.4.3 Conceptually Comparing Alignment Cultural Differences Between Belgium and the Netherlands

As a first empirical exploration of the influence of national cultures on alignment, we compared the results of alignment maturity assessments in Belgium and the Netherlands. The selection of Belgium and the Netherlands was inspired by the substantial differences on three of the four Hofstede's culture variables by these neighboring countries. Figure 3.15 shows these scores.

The analysis of the relationship between Hofstede's dimensions of culture on Luftman's variables of alignment maturity can now be made specific for the differences between Belgium and the Netherlands.

3.4.3.1 Power Distance Index

PDI—Communications maturity: The Belgium PDI is moderately high, whereas the PDI of the Netherlands can be classified as moderately low. Therefore it should be expected that the Netherlands scores higher in Communications maturity than Belgium.

Expectation: Comm M NL > Comm M BE

PDI—Value measurement maturity: The relatively low PDI score of the Netherlands should result in a lower Value measurement maturity, compared to Belgium.

Expectation: Value M NL < Value M BE

PDI—Governance maturity: Given the difference in PDI scores of Belgium and the Netherlands, it should be expected that Belgium scores higher in Governance maturity than the Netherlands.

Expectation: Gov M NL < Gov M BE

PDI—Partnership maturity: Given the difference in PDI scores of Belgium and the Netherlands, it should be expected that the Netherlands scores higher in Partnership maturity than Belgium.

Expectation: Par M NL > Par M BE

PDI—Scope and Architecture maturity: Given the lack of indications for this relationship, it is unclear how the difference in PDI scores of Belgium and the Netherlands reflect in the Scope and Architecture maturity scores.

Expectation: Arch M NL ? Arch M BE

PDI—Skills maturity: Given the difference in PDI scores for Belgium and the Netherlands, it should be expected that Dutch companies score higher on Skills maturity than Belgium companies.

Expectation: Sk M NL > Sk M BE

3.4.3.2 Individualism vs. Collectivism

Since Belgium and the Netherlands both score relatively high on the IDV factor, no specific difference in maturity score is expected on this variable.

Expectation: All variables NL ≈ All variables BE

3.4.3.3 Masculinity vs. Femininity

MAS—Communications maturity: The Dutch culture can be classified as strong feminine, whereas Belgium takes on a middle position on this factor. This strengthens our earlier expectation that the Netherlands scores higher in Communications maturity than Belgium.

Expectation: Comm M NL > Comm M BE

MAS—Value measurement maturity: The difference in MAS scores in Belgium and the Netherlands can be expected to result in a higher Value measurement maturity for Belgium companies, compared to Dutch companies.

Expectation: Value M NL < Value M BE

MAS—Governance maturity: The difference in MAS scores in Belgium and the Netherlands strengthens the expectation that Belgium companies will show a higher Governance maturity score, compared to Dutch companies.

Expectation: Gov M NL < Gov M BE

MAS—Partnership maturity: The high feminine score of the Netherlands provides indication that Dutch companies should be expected to show a higher Partnership maturity score than Belgium companies.

Expectation: Par M NL > Par M BE

MAS—Scope and Architecture maturity: The high feminine score of the Netherlands can be expected to reflect in a relatively high score on Scope and Architecture maturity, compared to Belgium.

Expectation: Arch M NL > Arch M BE

MAS—Skills maturity: Given the different expected effects of masculinity/femininity on the Skills maturity score, it is not possible to specify an expectation for the difference between Belgium and Dutch culture on this factor.

Expectation: Sk M NL ? Sk M BE

3.4.3.4 Uncertainty Avoidance Index

UAI—Communications maturity: On UAI Belgium scores quite high and the Netherlands take a middle position. Again this indicates that the Netherlands is expected to score higher on Communications maturity than Belgium.

Expectation: Comm M NL > Comm M BE

UAI—Value measurement maturity: Given the high UAI score of Belgium again, this provides indication that Belgium companies should show a higher score on Value measurement maturity, compared to Dutch companies.

Expectation: Value M NL < Value M BE

UAI—Governance maturity: Given the high UAI score of Belgium, also this factor provides an indication that Belgium companies should be expected to show a higher Governance maturity score than Dutch companies.

Expectation: Gov M NL < Gov M BE

UAI—Partnership maturity: This factor again provides indication that the Netherlands should be expected to score higher on Partnership maturity than Belgium.

Expectation: Par M NL > Par M BE

UAI—Scope and Architecture maturity: Following Png's motivation (Png 2001), it should be expected that the high UAI score of Belgium reflects in a high score on Architecture maturity.

Expectation: Arch M NL < Arch M BE

UAI—Skills maturity: Given the high UAI score of Belgium, this provides support for the expectation that the Netherlands score higher on Skills maturity than Belgium companies.

Expectation: Sk M NL > Sk M BE

Based upon this analysis, the expectations for the differences between Belgium and the Netherlands can be summarized as shown in Fig. 3.16.

PDI	IND	MAS	UAI	Conclusion
Communications maturity				Communications maturity
Comm M NL >> Comm M BE	Comm M NL ? Comm M BE	Comm M NL >> Comm M BE	Comm M NL >> Comm M BE	NL > Communications maturity B
Value measurement maturity				Value measurement maturity NL < Value measurement maturity B
Value M NL < Value M BE	Value M NL ? Value M BE	Value M NL < Value M BE	Value M NL < Value M BE	Governance maturity NL < Governance maturity B
Governance maturity				Partnership maturity NL > Partnership maturity B
Gov M NL < Gov M BE	Gov M NL ? Gov M BE	Gov M NL < Gov M BE	Gov M NL < Gov M BE	Partnership maturity NL > Partnership maturity B
Partnership maturity				Scope & Architecture maturity
Par M NL > Par M BE	Par M NL ? Par M BE	Par M NL > Par M BE	Par M NL > Par M BE	Arch M NL ? Arch M BE
Arch M NL ? Arch M BE	Arch M NL ? Arch M BE	Arch M NL > Arch M BE	Arch M NL < Arch M BE	Undecided
Scope & Architecture maturity				Skills maturity
Sk M NL > Sk M BE	Sk M NL ? Sk M BE	Sk M NL ? Sk M BE	Sk M NL > Sk M BE	Sk M NL > Skills maturity B

Fig. 3.16 Summary of the expected differences between Belgium and the Netherlands

3.4.4 Empirically Comparing Alignment Cultural Differences Between Belgium and the Netherlands

For this study, three Dutch companies and three Belgium companies in the financial services sector (banks, insurance companies, etc.) were selected. The choice for the financial services sector was made because among different industries, financial services, together with manufacturing and retailing, is the first industry to use information technologies and as such is already more matured in these domains, making empirical research interesting (Chiasson and Davidson 2005). To avoid bias by the overall alignment maturity, the participating companies were selected to have matching total maturity scores (deliberate sampling, Yin 2002).

Figure 3.17 shows the participants of the study. In each of the organizations, 6–11 business and IT managers completed the survey. Comparing the maturity scores assigned by business and IT per organization reveals that for most organizations the difference between the business and IT rating was not large.

<i>Company</i>	<i># Employees</i>	<i># Respondents</i>
Dutch companies		
Merchant Bank	500-1000	8
Investment Bank	250-500	9
Insurance company	>5000	6
Belgium companies		
Bank / Insurance	>5000	11
Bank	>5000	9
Insurance broker	500-1000	8

Fig. 3.17 Participants in the study

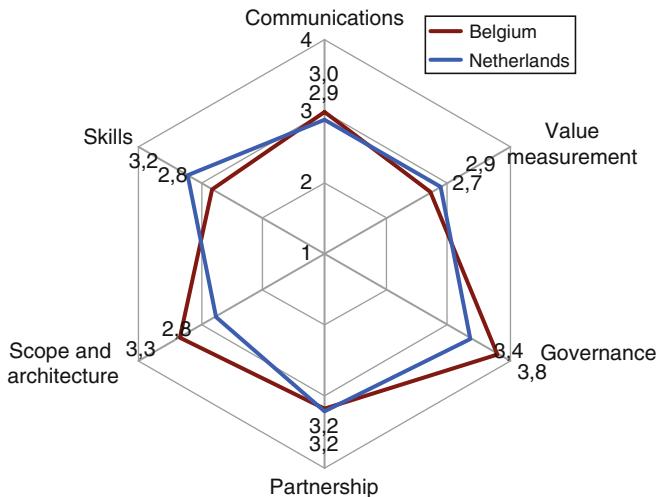


Fig. 3.18 Alignment maturity scores of the Belgium and Dutch participants

Figure 3.18 shows the overall average results of the alignment maturity assessments of the Belgium and Dutch participants. From this graph, some differences are immediately clear, specifically for “skills,” “governance,” and “scope and architecture.” Figure 3.19 shows the results on a deeper level. Based upon these differences, the following analysis can be made.

3.4.4.1 Communications Maturity

Average maturity of Belgium participants: 3.0.

Average maturity of Dutch participants: 2.9.

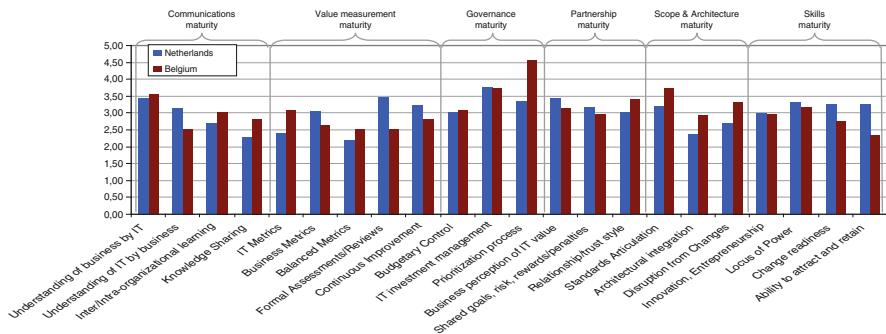


Fig. 3.19 Detailed BIA maturity scores of the Belgium and Dutch participants

The scores of the Belgium participants and that of the Dutch participants do not show a lot of difference, also on the level of the individual assessment items shown in Fig. 3.19. The expected difference is therefore not confirmed.

3.4.4.2 Value Measurement Maturity

Average maturity of Belgium participants: 2.7.

Average maturity of Dutch participants: 2.9.

The scores of the Belgium participants and that of the Dutch participants on this variable show some difference. On the more detailed level, a substantial difference is shown on the item “Formal assessments/reviews.” The direction of the difference however is opposite to the expectation. The expected difference is therefore not confirmed.

3.4.4.3 Governance Maturity

Average maturity of Belgium participants: 3.8.

Average maturity of Dutch participants: 3.4.

On this variable of alignment maturity, the results show the expected difference that the Belgium participants score higher than the Dutch participants. On the more detailed level, it becomes clear that especially the prioritization process is scored significantly different. The expected difference is therefore confirmed.

3.4.4.4 Partnership Maturity

Average maturity of Belgium participants: 3.2.

Average maturity of Dutch participants: 3.2.

The scores of the Belgium participants and that of the Dutch participants on this variable are equal. The expected difference is therefore not confirmed.

3.4.4.5 Scope and Architecture Maturity

Average maturity of Belgium participants: 3.3.

Average maturity of Dutch participants: 2.8.

On this variable, the expectation was undecided. The results show a remarkably higher score of the Belgium participants than that of the Dutch participants. On the more detailed level, this difference shows on all items.

3.4.4.6 Skills Maturity

Average maturity of Belgium participants: 2.8.

Average maturity of Dutch participants: 3.2.

On this variable, the results show the expected difference that the Dutch participants score a higher maturity than the Belgium participants. On the more detailed level, it becomes clear that this difference shows on all items, but most strongly on “Ability to attract and retain” and “Change readiness.” The expected difference is confirmed.

Figure 3.20 shows the summary of the results of this exploratory study.

Expectation	Result	
Communications maturity	Comm M NL > Comm M BE	Comm M NL ≈ Comm M BE
Value measurement maturity	Value M NL < Value M BE	Value M NL ≈ Value M BE
Governance maturity	Gov M NL < Gov M BE	Gov M NL < Gov M BE
Partnership maturity	Par M NL > Par M BE	Par M NL = Par M BE
Scope & Architecture maturity	Arch M NL ? Arch M BE	Arch M NL < Arch M BE
Skills maturity	Sk M NL > Sk M BE	Sk M NL > Sk M BE

Fig. 3.20 Summary of expectations and results

Summary

There is no universal way to measure business/IT alignment in literature. Many researchers have developed models that attempt to capture the complex alignment construct as complete as possible. Each measurement model has its own approach, and as a result, it is very difficult to compare results of alignment studies. Some potential approaches are described in this chapter, all having their strengths and weaknesses. In the end, it is important to select the approach that is most suited for the type of activity or research one is trying to do.

This chapter also reported on the results of a study that illustrates the relationship between business/IT alignment and Enterprise Governance of IT, using on Luftman's maturity model as proxy to measure alignment. It is concluded that well-aligned organization clearly adopted more mature IT governance practices as compared to poorly aligned organizations.

Finally, this chapter also explored the potential influence of culture on alignment differences. Our first empirical exploration provided support for the existence of differences in alignment maturity between countries based on the Hofstede framework.

Study Questions

1. Discuss how business/IT alignment can be measured and determine which is the most practical approach.
2. Explain how business/IT alignment can be measured through Luftman's model.
3. Explain the relationship between Enterprise Governance of IT and business/IT alignment.
4. Discuss the impact of cultural differences on business/IT alignment maturity.

Acknowledgement We want to express our gratitude to Dr. Gilbert Silvius for working with us on understanding the cultural dimension of business/IT alignment.

References

- Batenburg, R. (2007). E-procurement adoption by European firms: A quantitative analysis. *Journal of Purchasing and Supply Management*, 13, 182–192.
- Chiasson, M. W., & Davidson, E. (2005). Taking industry seriously in information systems research. *MIS Quarterly*, 29(4), 591–605.
- 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.
- Gefen, D., & Straub, D. (1997). Gender differences in the perception & use of e-mail: Extension to the technology acceptance model. *MIS Quarterly*, 21(4), 389–400.

- Hall, E. T. (1976). *Beyond culture*. New York: Anchor Press.
- Hofstede, G., & Bond, M. H. (1984). Hofstede's culture dimensions an independent validation using rokeach's value survey. *Journal of cross-cultural psychology*, 15(4), 417–433.
- Hofstede, G. (1991). *Culture and organizations: Software of the mind*. London, England: McGraw Hill.
- Hofstede, G. (2000). The information age across cultures. In *Proceedings of 5th AIM Conference—Information Systems and Organizational Change*. CD-Rom, 10pp.
- Livonen, M., Sonnenwald, D. H., Parma, M., & Poole-Kober, E. (1998). Analyzing and understanding cultural differences: Experiences from education in library and information studies. In *Proceedings of the 64th IFLA General Conference*, Amsterdam, The Netherlands.
- Luftman, J. (2000). Assessing business-IT alignment maturity. *Communications of the Association for Information Systems*, 4, Article 14.
- Luftman, J. N. (2007). An update on business-IT alignment: "A line" has been drawn. *MIS Quarterly*, 6(3), 165.
- Parker, M., Benson, R., & Trainor, H. (1988). *Information economics: Linking business performance to information technology*. London, England: Prentice Hall.
- Png, I. P. L., Tan, B. C. Y., & Wee, K. L. (2001). Dimensions of national culture and corporate adoption of IT infrastructure. *IEEE Transactions on Engineering Management*, 48(1), 36–45.
- Sabherwal, R., & Chan, Y. (2001). Alignment between business and IS strategies: A study of prospectors, analyzers and defenders. *Information Systems Research*, 12(1), 11–33.
- Silvius, G., De Haes, S., & Van Grembergen, W. (2010). Explorative study on the influence of national cultures on business/IT alignment maturity. *International Journal on IT/Business Alignment and Governance*, 1(2), 26–46.
- Sørnes, J.-O., Stephens, K., Sætre, A. S., & Browning, L. D. (2004). The reflexivity between ICTs and business culture: Applying Hofstede's theory to compare Norway and the United States. *Informing Science Journal*, 7, 1–30.
- Straub, D. W., Keil, P., & Brenner, A. (1997). Testing the technology acceptance model across cultures: A three country study. *Information & Management*, 31(1), 1–11.
- Turel, O., & Bart, C. (2014). Board-level IT governance and organizational performance. *European Journal of Information Systems*, 23, 223–239.
- van Birgelen, M., Ruyter, K. D., Jong, A. D., & Wtzels, M. (2002). Customer evaluations of after-sale service contact modes: An empirical analysis of national culture's consequences. *International Journal of Research in Marketing*, 19, 43–64.
- Van Grembergen, W., De Haes, S., & Van Brempt, H. (2007). How does the business drive IT? Identifying, prioritising and linking business and IT goals. *Information Systems Control Journal*, 6, 54–56.
- Veiga, J. F., Floyd, S., & Dechant, K. (2001). Towards modelling the effects of national culture on IT implementation and acceptance. *Journal of Information Technology*, 16(3), 145–158.
- Walls, J. (1993). Global networking for local development: Task focused and relationship focused in crosscultural communication. In L. Harasim (Ed.), *Global networks: Computers and international communication*. Cambridge, MA: MIT.
- Weill, P., & Broadbent, M. (1998). *Leveraging the new infrastructure: How market leaders capitalize on information technology*. Boston: Harvard Business School Press.
- Weill, P., & Ross, J. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Boston: Harvard Business School Press.
- Yin, R. K. (2002). *Case study research: Design and methods* (Applied Social Research Methods 3rd ed.). Thousand Oaks, CA: Sage.

Chapter 4

IT-Enabled Value

Abstract Previous chapters described what Enterprise Governance of IT is about and how it relates to business/IT alignment. The third component of the cascade introduced in Chap. 1 is related to the value question, or in other words, are we getting the benefits out of IT-enabled initiatives? In this chapter, we briefly discuss the productivity paradox and introduce two important management instruments that are helpful in managing and realizing IT-enabled value: the business case and the IT balanced scorecard.

4.1 The IT Black Hole

Investments in IT are growing extensively, and business managers often worry that the benefits of IT investments might not be as high as expected. The same worry accounts for the perceived ever-increasing total cost of the IT department, without clear evidence of the value derived from it. This phenomenon is called the “IT black hole”: large sums go in, but no returns (seem to) come out.

Getting business value from IT and especially measuring that value are therefore important governance domains. This should be a shared responsibility between business and IT and should take both tangible and intangible costs, benefits and risks into account. Or, in other words, measuring and managing IT-related value should provide answers to questions such as (Van Grembergen & De Haes 2005a, b):

- If I spend a dollar/euro extra on IT, what do I get back?
- How does my IT benchmark against competitors?
- Do I get back from IT what was promised?
- How do I learn from past performance to optimize my organization?
- Is my IT implementing its strategy, in line with the business strategy?
- ...

In Sect. 4.2, we look at how to demonstrate, measure, and manage the value of a single IT-enabled investment through the business case process. In Sect. 4.3 of this chapter, we will discuss how to demonstrate, measure, and manage the performance and value of the IT department using the balanced scorecard as instrument.

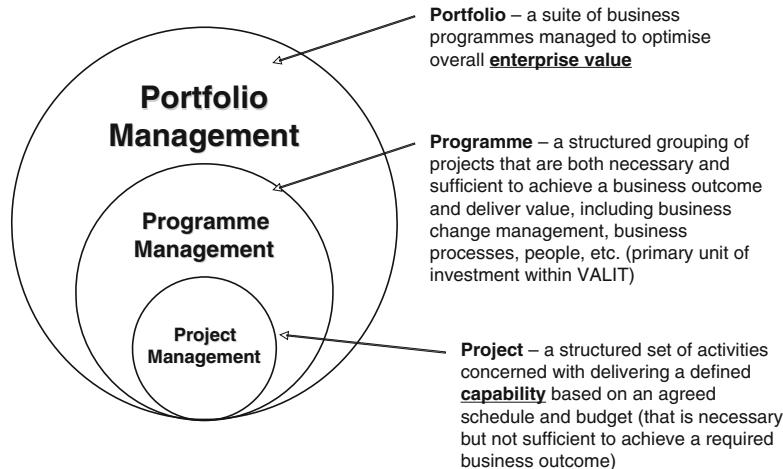


Fig. 4.1 Project, programmes, and portfolios ISACA, 2008, Val IT 2, online available at www.isaca.org

In support of this chapter (and by extension the whole book), we provide some definitions as we observe that organizations often have different interpretations regarding what is meant by an IT “project,” a “programme” and a “portfolio.” We propose definition as visualized in Fig. 4.1.

A project is a structured set of activities concerned with the delivery of a defined technical capability based on an agreed schedule and budget. Projects are defined at the level of the delivery of IT applications and solutions, such as a CRM application or a new website, which are necessary but not sufficient to achieve a required business outcome. A programme is a structured grouping of projects that are both necessary and sufficient to achieve a business outcome and deliver value. A programme therefore is the combination of the “IT project” and all other business-related projects such as defining new business processes, providing training, managing change, etc. Finally, the suite of investment programmes, including also those with no IT involvement, is to be managed as a portfolio in order to optimize to total value creation for the organization.

4.2 The Business Case Process

Academic scholars seem to agree that a business case is a formal document that provides a structured overview of information about a potential investment. All useful information is bundled in the business case and relevant calculations are described to provide a rationale and justification for the potential investment (Krell & Matook, 2009). The overall goal of a business case is consistently

described as to enable well-founded business decisions to make, let proceed, or stop the investment (ISACA, 2008; Post, 1992). As a result, we define a business case as a formal investment document with a structured overview of relevant information that provides a rationale and justification of an investment with the intent to enable well-founded investment decision-making (Maes, De Haes, & Van Grembergen, 2013).

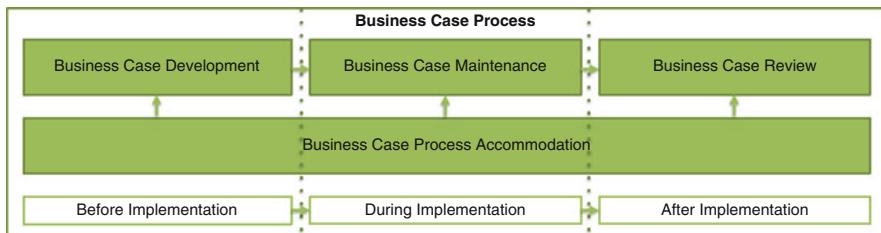
Many business cases which are developed to support the investment approval gather dust on a shelf afterwards (Franken, Edwards, & Lambert, 2009). Nonetheless, continuously using a business case throughout an entire investment life cycle can increase the adoption of the information system (IS) and is fundamental to benefit realization (Al-Mudimigh, Zairi, & Al-Mashari, 2001; Law & Ngai, 2007). Moreover, it is one of the major success factors for an investment and a source of a competitive advantage (Altinkemer, Ozcelik, & Ozdemir, 2011; Krell & Matook, 2009). Therefore, organizations should start to approach a business as a process instead of as a document. A process approach on business cases can be conceived as a business process which attempts to transform the formal business case document into a living document (Franken et al., 2009). We therefore define such a business case process as a set of logically related tasks that affect a business case and supports continuous business case usage with the intent to enable well-founded investment decision-making and to ultimately increase investment success (Maes, De Haes, & Van Grembergen, 2014).

A business case process runs in parallel with an investment life cycle, presented through a simplified three-phase-perspective: before, during, and after implementation. The conceptual model displayed in Fig. 4.2, is developed based on the literature review and presents a business case process consisting of three distinct but consecutive phases supported by an accommodating layer. These four components constitute together the business case process model and each component is defined in Fig. 4.2

In our research, we asked experts to give their opinion on the perceived effectiveness and perceived ease of implementation per business case practice.

Stakeholder attention is found to be very effective: both identifying their expectations (BCD03) and ensuring their active involvement (BCPA07) is positioned within the top three of highly effective practices. Indeed, stakeholders should be invited to participate in the development of business case and no investment should be approved without their active involvement (Matthews, 2004; Smith, McKeen, Cranston, & Benson, 2010). Communicating the business case to stakeholders is believed to be crucial in order to achieve their support and involvement (Luna-Reyes, Zhang, Gil-García, & Cresswell, 2005). They must be able to understand the business case, so it should be presented and communicated to them in an appropriate business language (Davenport et al., 2010; Sherif & Vinze, 2002). One expert concluded, “it is clear that personally, based on experience, I value the importance of stakeholder information, consultation, and commitment very high. It is a critical success factor for business case realisation.”

Another set of practices that are perceived to be highly effective deals with what the investment wants to realize. One expert clarifies: “It is of utmost importance to



Component	Definition: A set of logically related practices to...
<i>Business Case Development (BCD)</i>	identify relevant investment information that is integrated in a structured way with adequate and objective argumentation, in order to provide a rationale and justification of the initial investment idea.
<i>Business Case Maintenance (BDM)</i>	monitor whether the investment is implemented in accordance with the business case (e.g. objectives, changes, costs), and to update the business case with the prevailing reality (e.g. assumptions, risks).
<i>Business Case Review (BCR)</i>	monitor benefit realisation resulting from the utilisation of products and services, and to facilitate the evaluation of the overall investment success.
<i>Business Case Process Accommodation (BCA)</i>	facilitate an adequate execution of the business case process adjusted to the investment and organisational context.

Code	A business case is developed by...	Definition
BCD01	Capturing investment vision	Capture the investment vision and establish the appropriate investment context.
BCD02	Capturing business drivers	Capture the business challenges and opportunities that drive the investment and how they contribute to the achievement of the organisational strategy.
BCD03	Identifying stakeholder expectations	Identify the stakeholders' expectations, needs and requirements in terms of delivered benefits.
BCD04	Identifying technology opportunities	Identify proven and emerging technologies that support the business drivers and may realise the investment objectives.
BCD05	Identifying investment scope	Identify what will be done in the investment and what not, and explain why.
BCD06	Identifying investment assumptions	Identify realistic assumptions and their logic for business drivers, investment objectives, investment solution(s), benefits, and costs.
BCD07	Identifying investment objectives	Identify and categorise what objectives the investment should achieve.

Fig. 4.2 The business case process aligned with an investment life cycle. *Source:* Maes Kim, De Haes Steven, Van Grembergen Wim. Using a business case throughout an investment: an exploratory case study on a business case process, Proceedings of Americas Conference of Information Systems (AMCIS)—Chicago, 2013

BCD08	Identifying investment solution(s)	Identify what organisational and technological changes are required, design one or more alternative investment solutions and implementation scenarios, and assign change owners.
BCD09	Identifying investment benefits	Identify and categorise what benefits will be created by the investment based on relevant evidence, define their explicit measures and assign benefit owners.
BCD10	Identifying investment costs	Identify and categorise what costs will be created by the investment based on relevant evidence, and define their explicit measures.
BCD11	Identifying investment risks	Identify and evaluate the impact and probability of investment risks and critical success factors, and determine preferred solutions to take a proactive approach.
BCD12	Developing benefits realisation plan	Develop a structured plan on when each benefit will be realised, in relevant phases and with appropriate consideration of organisational factors.
BCD13	Evaluating investment feasibility and viability	Evaluate the feasibility and viability of each alternative investment solution.
BCD14	Evaluating cost/benefit analysis	Capture identified investment costs and benefits with measures and values, and evaluate cost/benefit analysis to support the financial argumentation.
Code	maintained by...	Definition
BCM01	Monitoring business case relevance	Monitor the business drivers, objectives and assumptions, and control whether they are still relevant and realistic.
BCM02	Monitoring investment scope	Monitor the investment scope and realisation of changes, and control whether it is still in line with the business case relevance.
BCM03	Monitoring investment costs	Monitor whether the investment costs are consumed according to the scope and identified changes.
BCM04	Monitoring investment risks	Monitor the investment risks and evaluate their impact on the business case.
BCM05	Updating business case to react adequately	Update the business case frequently based on business case monitoring and identify adequate actions.
Code	reviewed by...	Definition
BCR01	Identifying objective evaluation criteria	Identify and communicate objective criteria with predefined weighting that help to evaluate the investment effectiveness and efficiency.
BCR02	Evaluating investment effectiveness	Monitor benefits realisation, and evaluate the contribution of investment objectives and changes.
BCR03	Evaluating investment efficiency	Evaluate the effort and costs that were consumed to realise the investment.

Fig. 4.2 (continued)

Code	A business case process accommodated by...	Definition
BCPA01	Establishing adaptable business case approach	Establish an adaptable business case approach according to investment and accept a growing maturation and granularity through its development and usage.
BCPA02	Establishing business case templates, training and guidance	Establish standard business case templates and tools, and accommodate training and guidance on what constitute business case practices and how to employ them adequately.
BCPA03	Establishing maximum objectivity in business case usage	Maximise objectivity to support well-founded and comparable decision-making without influence from politics, lobbying or institutional powers.
BCPA04	Establishing simple and dynamic business case usage	Describe and employ business case practices and its content in a simple, straightforward and dynamic manner to encourage their usage.
BCPA05	Establishing business case practices as standard approach	Establish and evangelise business case practices as a standard way of working.
BCPA06	Ensuring business case practice improvements	Ensure business case practice improvements further through experience and continuous learning.
BCPA07	Ensuring communication and involvement with stakeholders	Ensure clear communication and active involvement with all stakeholders in order to gain insight, commitment and ownership.
BCPA08	Ensuring stakeholder confirmation	Ensure formal confirmation from relevant stakeholders on the (updated) business case to increase their commitment.
BCPA09	Evaluating business case regularly	Evaluate all business case documents in order to make well-founded decisions to approve, let proceed or stop the investment.

Fig. 4.2 (continued)

(1) know exactly what problem you want to solve, (2) understand how this will be solved, and (3) obtain and maintain the desire to achieve this.” Although the latter refers mostly to the importance of stakeholder attention and involvement, the other two can directly be linked to BCD01, BCD02, BCD05, and BCD07. These four practices focus on the identification of the investment vision and what business

drivers will be tackled, what will be included in the investment scope or not, and which objectives should be realized. The development of a business case should start from these fundamental questions (Ward, Daniel, & Peppard, 2008). The business drivers explain the current internal and external issues that the organization is facing, which directly influence the investment vision. In one exploratory case study, we discovered that market circumstances demanded fast decision-making for investing, divesting, and restructuring business divisions. As the company's daily operations and supporting ERP system were too inflexible to enable this, they initiated a new worldwide ERP investment.

The consensus levels on perceived ease of implementation scores are much lower and many experts attributed a score of 3 to several practices (moderate ease-of). This demonstrates that experts have much more difficulty to agree on their ease of implementation. We observe two outliers that are perceived to be easy to implement (>70 % of experts): BCPA02 and BCM03. As BCPA02 deals with the establishment of business case templates, training and guidance (BCPA02), experts perceive that such documents are easy to be created and distributed among stakeholders. The fact that this practice has not received high consensus on its perceived effectiveness contradicts with Smith et al. (2010). In one case study, the authors found that "the creation of a standard business case template was a big early win" for the investments. Next, the monitoring of investment costs (BCM03) is perceived as easy to implement by 83 % of the experts (same score as effectiveness). Identifying costs (BCD10), which could be seen as the foundation of BCM03, was also perceived as easy to implement but did not reach high consensus on perceived effectiveness. It is found hard to comprehensively identify, forecast, and quantify costs (Goldschmidt, 2005; Powell, 1993), while we found in case studies that investment costs are relatively easy to be monitored on a frequent basis. This finding is somewhat surprising and contradictory, because the monitoring of costs is largely dependent upon a solid identification of what costs the investment will generate, and as such what costs should be monitored. We claim that not effectively performing the identification of costs will undoubtedly impact the effectiveness of the monitoring practice.

Very low consensus levels on ease of implementation were achieved for 25 practices. This finding should not come as a surprise as many organizations still struggle with business case usage (Jeffrey & Leliveld, 2004; Taudes, Feurstein, & Mild, 2000). Business cases are often developed on the IT side although the responsibility should be positioned on the business side (Beatty & Williams, 2006). IT people are less able to perform this job as they have difficulties to estimate the added value that comes from strategic and tactical business opportunities such as flexibility, service, and market innovation (Taudes et al., 2000). We conclude that a great discrepancy can be found between how effective most business case practices are perceived and the perception of their ease of implementation. This contrast signals to us an important urge to investigate how these practices can be better implemented in the future.

If the consensus level for perceived effectiveness and ease of implementation is averaged for the different process model components (see Fig. 4.3), we discern that most consensus is achieved for effectiveness on practices in the Business

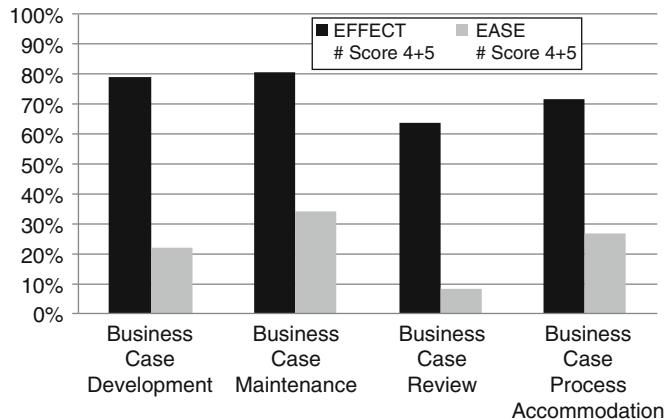


Fig. 4.3 Consensus levels on perceived effectiveness and perceived ease of implementation of business case practices per process model component (based on score 4 and 5 on Likert-scale)

Case Maintenance component, closely followed by those in the Business Case Development component. The consensus rate for Business Case Process Accommodation practices is still within the high consensus cut-off level ($>70\%$), while only 64 % of the experts perceive Business Case Review practices as effective. Practices from this component are also perceived lowest on ease of implementation. Although all four components receive a low to very low consensus rate on perceived ease of implementation, again practices from the Business Case Maintenance component achieve the highest rate. Hence, we might reason that organizations will achieve the highest return on effort when they implement the practices from the Business Case Maintenance component. Following up on the relevance of the business case is certainly important, according to (Al-Mudimigh et al., 2001), because the business drivers and objectives can be impacted by a shift in market, organizational, or technological issues. If an organization wants to understand how it needs to react on these changes, this impact should be investigated. This might require an update of the business case (Brown and Lockett, 2004). In case a dramatic change threatens the business case relevance, one should reassess the fundamental assumptions and perform a new cost-benefit analysis (Flynn, Pan, Keil, & Mähring, 2009; Lacovou & Dexter, 2004). We think experts perceive the effectiveness of these Business Case Maintenance practices as high as they possess the ability to have a direct impact on last-minute changes and to contribute greatly to the effects of ongoing investment decision-making. After all, a continuous reflection on, and update of, the business case throughout the entire investment life cycle is import to ultimate benefit realisation (Al-Mudimigh et al., 2001).

The lowest return might be expected from practices in the Business Case Review component, as they score lowest on both effectiveness and ease of implementation. Potentially, experts have reasoned that the job is done by then and that these practices

have no direct impact anymore on the final result. This is however not entirely true, because monitoring benefit realization is included in BCR02. Most probably, the practice has therefore achieved the highest consensus rate on effectiveness in its process model component. Together with the identification of objective evaluation criteria, it is the only practice that realizes the high consensus cut-off level of 70 %. Consistent with (Ashurst, Doherty, & Peppard, 2008), a set of evaluation criteria should be established in an objective manner and with prior agreement by the stakeholders. After the resulting products and services from the investment have officially been launched, benefit realization should be frequently monitored against the objective evaluation criteria (Fonstad & Robertson, 2006). In one case study, we found that the organization updated its benefit realization plan after the launch to be most in line with reality (including additional change request from during the project).

Assignment Box 4.1: Assessment of the Business Case Process

In case you have access to an organization: for a recently finalized IT-enabled investment, or a running investment, assess how the investment is being managed through the business case process. For each of the identified business case management practices in this section, assess (for example on a scale from 0 to 5), whether or not the organization is applying each of these practices. If possible, discuss your results in the context of the realized (or not realized) benefits of the investment under review.

4.3 The Balanced Scorecard

The IT BSC is becoming a popular tool to measure and manage the value of IT, with its concepts widely supported and dispersed by international consultant groups such as Gartner, IDC, and others. As a result of this interest, many real-life applications have been developed and are supported by software tools.

4.3.1 *IT BSC Core Concepts*

In the early nineties, Kaplan and Norton (1996) introduced the BSC at enterprise level. Their fundamental premise is that the evaluation of a firm should not be restricted to a traditional financial evaluation but should be supplemented with objectives and measures concerning customer satisfaction, internal processes, and the ability to innovate. Results achieved within these additional perspective areas should assure future financial results and drive the organization towards its strategic goals while keeping all

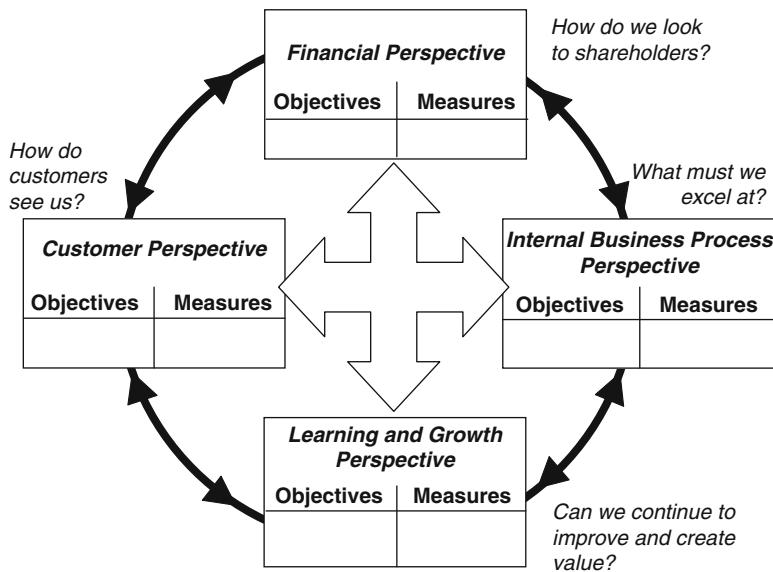


Fig. 4.4 Generic business balanced scorecard. Adapted from: Kaplan, R. and Norton, D. *The balanced scorecard: translating vision into action*, Harvard Business School Press, Boston, 1996

four perspectives in balance. For each of the four perspectives of the business BSC, Kaplan and Norton (1996) propose a three-layered structure, as shown in Fig. 4.4:

1. Mission (e.g., to become the customers' most preferred supplier)
2. Objectives (e.g., to provide the customers with new products)
3. Measures (e.g., percentage of turnover generated by new products)

The BSC can be applied to the IT function, its processes and projects. (Van Der Zee, 1999; Van Grembergen, Saull, & De Haes, 2003; Van Grembergen & Van Bruggen, 1997). To achieve that, the focus of the four perspectives of the business BSC needs to be translated, as shown in Fig. 4.5. The User Orientation perspective represents the user (internal or external) evaluation of IT. The Operational Excellence perspective represents the IT processes employed to develop and deliver the applications. The Future Orientation perspective represents the human and technology resources needed by IT to deliver its services over time. The Business Contribution perspective captures the business value created from the IT investments.

Again, each of these perspectives has to be translated into corresponding goals and metrics that assess the current situation. These assessments need to be repeated periodically and aligned with preestablished goals and benchmarks. Example metrics for the four perspectives are provided in Fig. 4.6.

To leverage the IT BSC as a management and alignment instrument, it should be enhanced with cause-and-effect relationships between measures. These relationships

USER ORIENTATION How do the users view the IT department?	CORPORATE CONTRIBUTION How does management view the IT department?
Mission to be the preferred supplier of information systems	Mission to obtain a reasonable business contribution of IT investments
Objectives <ul style="list-style-type: none"> ▪ preferred IT supplier ▪ partnership with users ▪ user-satisfaction 	Objectives <ul style="list-style-type: none"> ▪ control of IT expenses ▪ business value of the IT function ▪ business value of new IT projects
OPERATIONAL EXCELLENCE How effective and efficient are the IT processes?	FUTURE ORIENTATION How well is IT positioned to answer future challenges?
Mission to deliver effective and efficient IT applications and services	Mission to develop opportunities to answer future challenges
Objectives <ul style="list-style-type: none"> ▪ efficient software development ▪ efficient computer operations ▪ efficient help desk function 	Objectives <ul style="list-style-type: none"> ▪ training and education of IT staff ▪ expertise of IT staff ▪ research into emerging information technologies

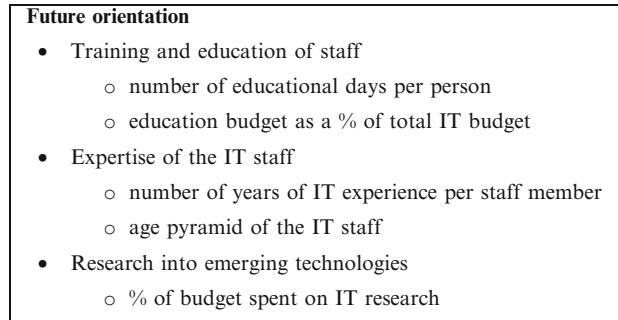
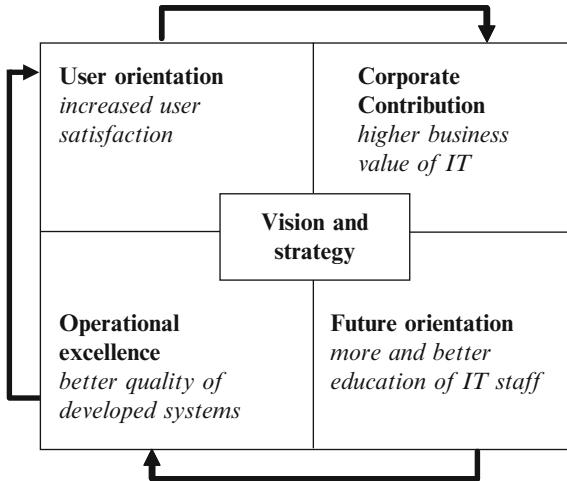
Fig. 4.5 Generic IT balanced scorecard

are articulated by two types of measures: outcome measures (or lag indicators) and performance drivers (or lead indicators). A well-developed scorecard should contain a good mix of these two metrics. Outcome measures without performance drivers do not communicate how they are to be achieved. And performance drivers without outcome measures may lead to significant investment without a measurement indicating whether the chosen strategy is effective. A good example of a cause-and-effect relationship, defined throughout the whole scorecard is shown in Fig. 4.7: more and better education of IT staff (future perspective) is an enabler (performance driver) for a better quality of developed systems (operational excellence perspective) that in turn is an enabler for increased user satisfaction (user perspective) that eventually must lead to a higher business value of IT (business contribution perspective).

The proposed IT BSC links with the business, mainly through the business contribution perspective. The relationship between IT and business can be more explicitly expressed through a cascade of scorecards. In Fig. 4.8 the relationship between IT scorecards and the business scorecard is illustrated. The IT Development BSC and the IT Operational BSC both are enablers of the IT Strategic BSC that in turn is the enabler of the Business BSC. This cascade of scorecards becomes a linked set of measures that will be instrumental in aligning IT and business strategy and that will help to determine how business value is created through IT.

Corporate contribution
<ul style="list-style-type: none"> • Control of IT Expenses <ul style="list-style-type: none"> ◦ percentage over or under IT budget ◦ allocation to different budget items ◦ IT budget as a percentage of turnover ◦ IT expenses per staff member • Business Value of the IT function <ul style="list-style-type: none"> ◦ percentage of the development capacity engaged in strategic projects ◦ relationship between new developments / infrastructure investments / replacement investments • Business Value of new IT Projects <ul style="list-style-type: none"> ◦ financial evaluation based on ROI, NPV, IRR, PB ◦ business evaluation based on Information Economics
User Orientation
<ul style="list-style-type: none"> • Preferred IT Supplier <ul style="list-style-type: none"> ◦ percentage of applications managed by IT ◦ percentage of applications delivered by IT • Partnership with users <ul style="list-style-type: none"> ◦ index of user involvement in generating strat. applications ◦ index of user involvement in developing new applications • User Satisfaction <ul style="list-style-type: none"> ◦ index of user friendliness of applications ◦ index of user satisfaction
Operational excellence
<ul style="list-style-type: none"> • Efficient Software Development <ul style="list-style-type: none"> ◦ average days late in delivering software ◦ average unexpected budget increase ◦ percentage of projects performed within SLA ◦ percentage of maintenance activities • Efficient Computer Operations <ul style="list-style-type: none"> ◦ percentage unavailability of network ◦ response times per category of users ◦ percentage of jobs done within time • Efficient Help Desk Function <ul style="list-style-type: none"> ◦ average answer time of help desk ◦ percentage of questions answered within time

Fig. 4.6 Example metrics for IT balanced scorecard

**Fig. 4.6** (continued)**Fig. 4.7** Cause-and-effect relationships within the IT strategic balanced scorecard

4.3.2 Mini-Case

In this section, the development and implementation of an IT BSC within the Information Services Division (ISD) of a Canadian tri-company financial group consisting of Great-West Life, London Life and Investors Group (hereafter named The Group) is described and discussed.

4.3.2.1 Company Introduction

The Great-West Life Assurance Company, London Life and Investors Group are members of the Power Financial Corporation group of companies, with London Life as a wholly owned subsidiary of The Great-West Life Assurance Company. In 2001,

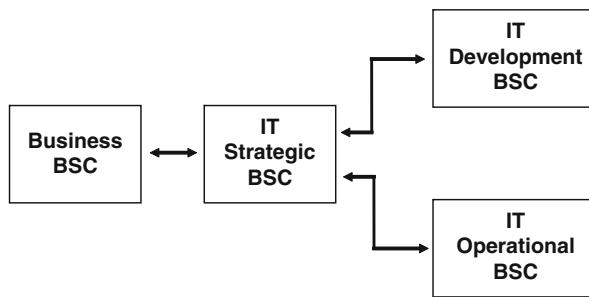


Fig. 4.8 Cascade of balanced scorecards

MacKenzie financial was also acquired by the Power Financial Corporation Group, but as the IT balanced scorecard project does not cover this company, MacKenzie's organization and IT division will not be taken into account in this article.

The Great-West Life Assurance Company is an international corporation offering life insurance, health insurance, retirement savings, specialty reinsurance and general insurance, primarily in Canada and the United States. Great-West serves the financial security needs of more than 13 million people in Canada and the United States. Great-West has more than \$86.9 billion (all figures in this article are in Canadian dollars) in assets under administration and \$477 billion of life insurance in force. Founded in Winnipeg in 1891, Great-West is now a leading life and health insurer in the Canadian market in terms of market share.

London Life was founded in Ontario in 1874 and has the leading market share of individual life insurance in Canada. London Life markets life insurance, disability insurance, and retirement savings and investment products through its exclusive sales force. The company is a supplier of reinsurance primarily in the United States and Europe, and is a 39 % participant in a joint venture life insurance company Shin Fu in Taiwan. London Life has more than \$30 billion assets under administration and \$142.6 billion of life insurance in force.

Investors Group, with its corporate headquarters in Winnipeg, was founded more than 70 years ago. Investors Group is Canada's leading provider of mutual funds, offering a wide spectrum of funds, including those created through strategic partnerships with some of the best known Canadian and international investment management firms. It also offers a wide range of insurance and mortgage options, and currently has \$17.1 billion of life insurance coverage in force through three different carriers, and administers with more than \$7.6 billion of primarily residential mortgages. Investors Group manages assets of \$40.5 billion.

The trend in financial services industry consolidation was a motivating factor behind the acquisition of London Life by Great-West Life and the merger of the IT divisions of the three companies in November 1997. At that time, the tri-company IT expenditures had exceeded \$200 million. The ability to reduce these costs and to achieve true synergies and economies of scale within the IT operations was clearly a driver and opportunity for the companies to realize. The merger enabled single

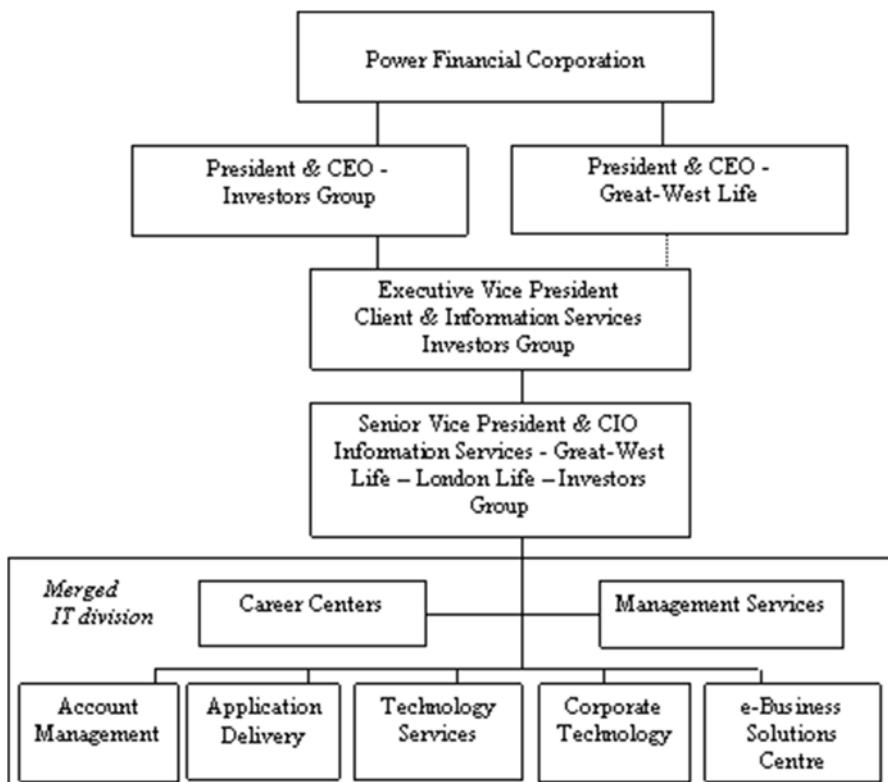


Fig. 4.9 Organization chart

system solutions across all three companies to be explored and implemented as well as single operational processes. Forming a tri-company shared services organization positioned management to:

- Achieve world-class status as an information services group
- Maximize purchasing power and operating efficiency
- Leverage technology investments
- Optimize technical infrastructure and application support costs

Figure 4.9 depicts the current IT organizational structure of the merged IT division, which employed 812 full-time/part-time employees in 2002. Also the position of the IT division relative to the higher reporting levels is indicated. *Application Delivery* and *Technology Services* are respectively the traditional IT department's Systems Development and Operations of the combined organizations. *Application Delivery* is separated from account management and people management in order to focus on continuous improvement of delivery performance. *Account Management* is the linkage with the clients/users. This component ensures effective communication and translation of business needs into IT processes and educates users on the IT

corporate agendas. Account Management employs IT generalists who provide IT insights into business strategy and decision-making. *Career Centers* are focused on the professional development of IT people and ensure attention to people issues in order to reduce turnover of talented IT employees. *Corporate Technology* enables the development of a common architecture and provides technology directions. The *eBusiness Solution Center* works on the introduction of new technologies that enable eBusiness solutions for The Group. *Management Services* focuses on running IT as a business and ensures effective financial management and management reporting including IT scorecard reporting.

4.3.2.2 IT BSC Project and Its Organization

Before the merger, the CIO of Great-West Life (who is the present CIO of the merged IT division), began focusing on the scorecard as a (potentially) effective measurement tool. His objective was to ensure that IT was fairly evaluated. In his own words: “Through the balanced scorecard I would know what was important to the business and I would not fall victim to the early termination syndrome. Or at least I would have a better chance of survival.”

However, once the three companies came together through the acquisition and merger of the IT groups, the stakes were raised considerably. Now, the IT division had exposures on multiple fronts with stakeholders who were concerned about the perceived loss of control over their vital IT services. This prompted an executive request for a formal measure of factors to measure IT success. The response of the merged IT division was to formalize the criteria into a new and extended IT scorecard based on the experiences gained within Great-West Life.

Senior management of all the three companies questioned the benefits of huge investments in IT and how more value might be achieved through better alignment of business strategy and IT strategy. Within The Group the specific concerns for the different stakeholders were (Fig. 4.10):

The concepts of the balanced scorecard and its application to information technology were discovered through an internet search primarily through the web site of the IT Governance Institute (www.itgi.org). Departing from this web site, relevant publications on the IT Balanced Scorecard from academics and practitioners were identified and consulted. It was believed that the scorecard could provide an answer to the key questions of the different stakeholders.

The formal development of the IT balanced scorecard began in 1998 and from the start the objectives were clearly stated:

- Align IT plans and activities with business goals and needs
- Align employees' efforts toward IT objectives
- Establish measures for evaluating the effectiveness of the IT organization
- Stimulate and sustain improved IT performance
- Achieve balanced results across stakeholder groups

Stakeholders	Key questions
Board of Directors Executive Management Committee	Does IT support the achievement of business objectives? What value does the expenditure on IT deliver? Are IT costs being managed effectively? Are IT risks being identified and managed? Are targeted inter-company IT synergies being achieved?
Business unit executives	Are IT's services delivered at a competitive cost? Does IT deliver on its service level commitments? Do IT investments positively affect business productivity or the customer experience? Does IT contribute to the achievement of our business strategies?
Corporate compliance internal audit	Are the organization's assets and operations protected? Are the key business and technology risks being managed?
IT Organization	Are proper processes, practices and controls in place? Are we developing the professional competencies needed for successful service delivery? Are we creating a positive workplace environment? Do we effectively measure and reward individual and team performance? Do we capture organizational knowledge to continuously improve performance? Can we attract/retain the talent we need to support the business?

Fig. 4.10 IT concerns of the different stakeholders

At the beginning of the implementation period (December 1999), the scorecard effort was not yet approached as a formal project and as a result, progress had been somewhat limited. In 2000 the formality of the project was increased and the CIO (Information Services Executive) was appointed as sponsor. In 2001, a project manager/analyst was formally assigned to the IT balanced scorecard project.

4.3.2.3 Building the IT BSC

It was recognized by the CIO that building an IT BSC was meaningful under two conditions which required (a) a clearly articulated business strategy, and (b) the new Information Services Division moving from a commodity service provider to a strategic partner. The newly constructed ISD is viewed as a strategic partner. During several meetings between IT and executive management, the vision, strategy, measures of success and value of IT were jointly created. Typically, pure business objectives were used as the standard to assess IT. The vision and strategy of ISD were defined as:

- ISD is a single IT organization focused on developing world-class capabilities to serve the distinct customer needs of its three sponsoring companies.
- ISD operates as a separate professional services business on a full recovery, non-profit basis.
- ISD supports the achievement of company strategies and goals through the industry consolidation period.
- ISD becomes the “supplier of choice” of information services.
- ISD establishes a forward looking enterprise architecture strategy which enables the use of technology as a competitive edge in the financial service market place.
- ISD becomes the “employer of choice” for career-oriented IT professionals in the markets in which ISD and The Group operate.

These issues go to the heart of the relationship between IT and the business and will be reflected in the IT strategic balanced scorecard as is illustrated in Figs. 4.11 and 4.12. Figure 4.11 shows the perspective questions and mission statements for the four quadrants: corporate contribution, customer orientation, operational excellence, and future orientation. Figure 4.12 displays the objectives for each perspective.

4.3.3 Corporate Contribution Perspective

The Corporate contribution perspective evaluates the performance of the IT organization from the viewpoint of executive management, the Board of Directors, and the shareholders, and provides answers to the key questions of these stakeholders concerning IT governance (cf. Fig. 4.10). The key issues, as depicted by Fig. 4.12, are business/IT alignment, value delivery, cost management, risk management, and intercompany synergy achievement. Benchmarks have been used where an objective standard was available or could be determined in most cases from external sources.

CUSTOMER ORIENTATION	CORPORATE CONTRIBUTION
<p><i>Perspective question</i></p> <p>How should IT appear to business unit executives to be considered effective in delivering its services?</p> <p><i>Mission</i></p> <p>To be the supplier of choice for all information services, either directly or indirectly through supplier relationships.</p>	<p><i>Perspective question</i></p> <p>How should IT appear to the company executive and its corporate functions to be considered a significant contributor to company success?</p> <p><i>Mission</i></p> <p>To enable and contribute to the achievement of business objectives through effective delivery of value added information services.</p>
OPERATIONAL EXCELLENCE	FUTURE ORIENTATION
<p><i>Perspective question</i></p> <p>At which services and processes must IT excel to satisfy the stakeholders and customers?</p> <p><i>Mission</i></p> <p>To deliver timely and effective IT services at targeted service levels and costs.</p>	<p><i>Perspective question</i></p> <p>How will IT develop the ability to deliver effectively and to continuously learn and improve its performance?</p> <p><i>Mission</i></p> <p>To develop the internal capabilities to continuously improve performance through innovation, learning and personal organizational growth.</p>

Fig. 4.11 Perspective questions and mission statements of the IT strategic scorecard

The main measurement challenges are with the areas of business/IT alignment and the value delivery. Currently, *business/IT alignment* is measured by the approval of the IT operational plan and budget. Although not a discrete measure of alignment, the approval process within the Group is particularly thorough and as a result is accepted by business executives as a good indicator. All aspects of development,

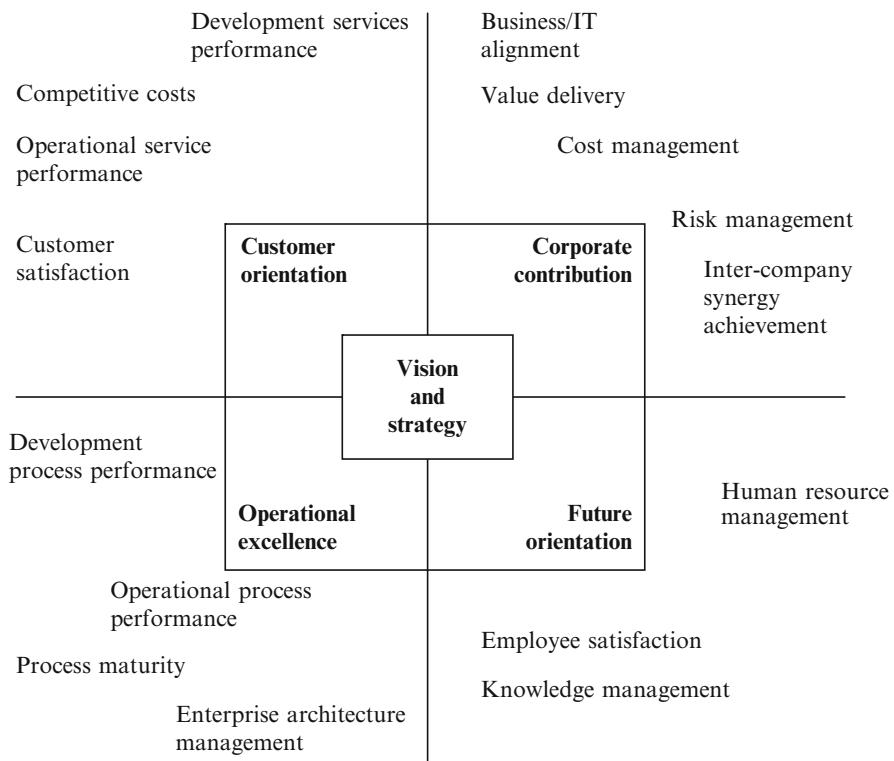


Fig. 4.12 IT strategic scorecard framework

operations, and governance/support services are examined and challenged to ensure they are essential to achieving business objectives or supporting the enabling IT strategy.

In the *value delivery* area, the performance of a specific IT services group delivering to a specific business unit (e.g., “group insurance” services) is measured. For each business unit, specific metrics are and/or will be defined. The ultimate responsibility for achieving and measuring the business value of IT rests with the business and is reflected in the business results of the individual lines of business in different ways, depending on the nature of value being sought.

Cost management is a traditional financial objective and is in the first place measured through the attainment of expense and recovery targets. The expenses refer to the costs that the IT organization has made for the business, and the recovery refers to the allocation of costs to IT services and the internal charge back to the business. All IT costs are fully loaded (no profit margin) and recovered from the lines of business on a fair and equitable basis as agreed to by the companies’ CFOs. Comparisons with similar industries will be drawn to benchmark these metrics. Next to this, IT unit costs (e.g., application development) will be measured and compared to the “top performing levels” benchmark provided by Compass.

The development of the *risk management* metrics is the priority for the upcoming year. At this moment, the results of the internal audits are used and benchmarked against criteria provided by OSFI, the Canadian federal regulator in the financial services sector. The execution of the Security Initiative and the delivery of a Disaster Recovery Assessment need to be accomplished in the upcoming year. This will enable the business to get an insight on how well they are prepared to respond to different disaster scenarios.

Synergy achievement is measured through the achievement of single system solutions, targeted cost reductions, and the integration of the IT organizations. This measure is very crucial in the context of the merger of the three IT organizations in the sense that it enables a post evaluation of this merger and demonstrates to management whether the new IT organization is effective and efficient. The selection of single system solutions was a cooperative effort between business leaders and IT staff, resulting in a “Target State Architecture” depicting the target applications architecture. The synergy targets were heavily influenced by the consulting firm (Bain & Co.) that was used to assist in evaluating the London Life acquisition and the tri-company IT merger potential. The consultants suggested specific dollar reduction targets for technology services (IT operations) and application delivery services (IT development) largely based on norms they had developed from their previous merger and acquisition work. The approval of the Target State Architecture plan and the attainment of the targeted integration cost reductions will be measured. The IT organization integration metric refers to the synergies within the IT organization, e.g., is there one single service desk for the three companies or are there three different ones? (Fig. 4.13).

4.3.4 Customer Orientation Perspective

The Customer orientation perspective evaluates the performance of IT from the viewpoint of internal business users (customers of IT) and, by extension the customers of the business units. It provides answers to the key questions of these stakeholders concerning IT service quality (cf. Fig. 4.10). As shown in Fig. 4.12, the issues this perspective focuses on are competitive costs, development services performance, operational services performance, and customer satisfaction.

In the *Customer satisfaction* area, the IT BSC of the merged IT organization is relying on annual interviews with key business managers. It is the intent to set up one generic survey, which can be reused, with relevant questions that cover the topics mentioned in Fig. 4.12.

Insight into the *competitive costs* area can demonstrate to the business how cost competitive the IT organization is compared to other (e.g., external) parties. This insight is realized by measuring the attainment of IT unit cost targets and the blended labor rate. This rate model provides an overall single rate for any IT professional who is appointed to the business. The competitive cost measures are benchmarked against Compass’s operational “Top Performing level” and against the offerings of commercial IT service vendors (market comparisons).

Objective	Measures	Benchmarks
Business/IT alignment	- Operational plan/budget approval	- Not applicable
Value delivery	- Measured in business unit performance	- Not applicable
Cost management	- Attainment of expense and recovery targets - Attainment of unit cost targets	- Industry expenditure comparisons - Compass operational 'top performance' levels
Risk management	- Results of internal audits - Execution of Security Initiative - Delivery of disaster recovery assessment	- OSFI sound business practices - Not applicable - Not applicable
Inter-company synergy achievement	- Single system solutions - Target state architecture approval - Attainment of targeted integration cost reductions - IT organization integration	- Merger & Acquisition guidelines - Not applicable - Not applicable - Not applicable

Fig. 4.13 Corporate contribution perspective

Development services performance measures are project oriented using attributes such as goal attainment, sponsor satisfaction, and project governance (i.e., the way the project is managed). These data are mostly captured by interviews with key managers. The most effective time to establish the basis for these (project) development measures is at the point where business cases are being prepared and projects are evaluated. Each IT project initiative will be evaluated by the IS Executive Committee in which IT and business managers determine—based on the business drivers, budget, and state architecture compliance—which projects need to be executed. When a project is approved, the project manager defines clear targets for cost, schedule, quality, scope, and governance. The quantitative data (e.g., budget) are reported throughout the lifecycle of the project. After completion of the project, the quantitative and qualitative data are evaluated during the major project review and the main success drivers, delivery issues, and lessons learned are documented.

In terms of *Operational service performance*, IT management measures achievement against targeted service levels. For each operational unit (e.g., data center),

Objective	Measures	Benchmarks
Customer satisfaction	<ul style="list-style-type: none"> - Business unit survey ratings: <li style="margin-left: 20px;">- Cost transparency and levels <li style="margin-left: 20px;">- Service quality and responsiveness <li style="margin-left: 20px;">- Value of IT advise and support <li style="margin-left: 20px;">- Contribution to business objectives 	- Not applicable
Competitive costs	<ul style="list-style-type: none"> - Attainment of unit cost targets <li style="margin-left: 20px;">- Blended labour rates 	<ul style="list-style-type: none"> - Compass operational 'Top Level Performing' levels <li style="margin-left: 20px;">- Market comparisons
Development services performance	<ul style="list-style-type: none"> - Major project success scores <li style="margin-left: 20px;">- Recorded goal attainment <li style="margin-left: 20px;">- Sponsor satisfaction ratings <li style="margin-left: 20px;">- Project governance rating 	- Not applicable
Operational services performance	- Attainment of targeted service levels	- Competitor comparisons

Fig. 4.14 Customer orientation perspective

average response time, service availability, and resolution time for incidents are rolled-up to these service performance metrics in the strategic balanced scorecard. The results are benchmarked against the performance of competitors Fig. 4.14.

4.3.5 *Operational Excellence Perspective*

The operational excellence scorecard provides the performance of IT from the viewpoint of IT management (process owners and service delivery managers) and the audit and regulatory bodies. The operational excellence perspective copes with

the key questions of these stakeholders and provides answers to questions of maturity, productivity, and reliability of IT processes (cf. Fig. 4.10). The issues that are of focus here, as displayed in Fig. 4.11, are development process performance, operational process performance, process maturity, and enterprise architecture management.

In relation to *development process performance*, function point-based measures of productivity, quality, and delivery rate such as number of faults per 100 installed function points and delivery rate of function points per month are defined. Benchmark data on industry performance will be gathered from a third party (e.g., Compass). In the operational process performance area, measures of productivity, responsiveness, change management effectiveness, and incident occurrence level are benchmarked against selected Compass studies (e.g., on data centers, client server, etc.).

The *process maturity* is assessed using the COBIT (Control Objectives for IT and related Technology) framework and maturity models (ITGI, 2000). The Group has identified 15 out the 34 priority processes that should have a maturity assessment in 2003 and the other processes will be measured later Fig. 4.15.

Enterprise architecture management deals with the IT responsibility to define an enterprise architecture which supports long-term business strategy and objectives and to act as a steward on behalf of business executives to protect the integrity of that architecture. Major project architecture approval measures the compliance of net new systems as they are proposed, developed, and implemented. Product acquisition compliance technology standards measure the adherence to detailed technology standards which are at the heart of minimizing technology diversity and maximizing intercompany technology synergies. The “State of the Infrastructure” assessment measures the degree to which IT has been able to maintain a robust and reliable infrastructure as required to deliver effectively to business needs. It does so by comparing each platform area against risk-based criteria for potential impact to business continuity, security, and/or compliance.

4.3.6 Future Orientation Perspective

The future orientation perspective shows the performance of IT from the viewpoint of the IT organization itself: process owners, practitioners, and support professionals. The future orientation perspective provides answers to stakeholder questions regarding IT’s readiness for future challenges (cf. Fig. 4.10). The issues focused on, as depicted in Fig. 4.12, are human resources management, employee satisfaction, and knowledge management. The metrics that will appear in the future orientation quadrant of the IT strategic balanced scorecard are in many cases the aggregated results of measures used in the unit scorecards (e.g., career center).

Human resource management is an objective that is tracked by comparing measures as described in Fig. 4.12 against predefined targets: the staff complement by skill type (number of people with a certain profile, e.g., systems analyst), staff turnover,

Objective	Measures	Benchmarks
Development process performance	- Function point measures of: - Productivity - Quality - Delivery rate	- to be determined
Operational process performance	- Benchmark based measures of: - Productivity - Responsiveness - Change management effectiveness - Incident occurrence levels	- Selected Compass benchmark studies
Process maturity	- Assessed level of maturity and compliance in priority processes within: - Planning and organization - Acquisition and implementation - Delivery and support - Monitoring	- To be defined
Enterprise architecture management	- Major project architecture approval - Product acquisition compliance to technology standards - “State of the infrastructure” assessment	- Not applicable

Fig. 4.15 Operational excellence perspective

staff “billable” ratio (i.e., hours billed/total hours salary paid; if this ratio can be increased, the IT organization can charge lower rates to the business for the IT assigned people), and professional development days per staff member.

Employee satisfaction is measured by using surveys with questions relating to compensation, work climate, feedback, personal growth, and vision and purpose.

Objective	Measures	Benchmarks
Human resource management	<ul style="list-style-type: none"> - Results against targets: <ul style="list-style-type: none"> - Staff complement by skill type - Staff turnover - Staff ‘billable’ ratio - Professional development days per staff member 	<ul style="list-style-type: none"> - Not applicable - Market comparison - Industry standard - Industry standard
Employee satisfaction	<ul style="list-style-type: none"> - Employee satisfaction survey scores in: <ul style="list-style-type: none"> - Compensation - Work climate - Feedback - Personal growth - Vision and purpose 	<ul style="list-style-type: none"> - North American technology dependent companies
Knowledge management	<ul style="list-style-type: none"> - Delivery of internal process improvements to ‘Cybrary’ - Implementation of ‘lessons learned’ sharing process 	<ul style="list-style-type: none"> - Not applicable - Not applicable

Fig. 4.16 Future orientation perspective

Benchmark data of North American technology-dependent companies are provided by a third party.

In the *knowledge management* area, the delivery of internal process improvements to the “Cybrary” is very important. The “Cybrary” refers to the intranet that all employees can assess for seeking and sharing knowledge. To measure improvements, metrics (e.g., number of hits per day on the Cybrary) still need to be developed. Closely linked to this, knowledge management is also measured by the implementation of the “lessons learned” sharing process. Here too, specific metrics still need to be developed Fig. 4.16.

4.3.6.1 Maturity of the Developed IT BSC

At the beginning of the project, the IT BSC was primarily focused on the operational level of the IT department. It was acknowledged from the beginning that this could not be the end result. Therefore, actions were started to go beyond the operational IT BSC and to measure the true value of IT at the business level. The Vice President Information Services emphasized: “The Balanced Scorecard gives a balanced view of the total value delivery of IT to the business. It provides a snapshot of where your IS organization is at a certain point in time. Most executives, like me, do not have the time to drill down into the large amount of information.”

The organization established two ways to demonstrate the business value, one at service delivery level and one at the IT strategy level. As will be illustrated hereafter, the goal is to evolve to an IT strategic BSC that shows how the business objectives are enabled by IT.

A cascade of balanced scorecards has been established to create a link between the scorecards at the unit level and the overall business objectives (see Fig. 4.17). A link between the IT BSC and the Business BSC is not yet implemented as there is currently no formal Business BSC for the Group. The scorecards at the unit level are classified into three groups: operational services scorecards (e.g., IT service desk scorecard), governance services scorecards (e.g., career center scorecard), and development services scorecards (e.g., application development scorecard). The measures of these unit scorecards are *rolled-up* or *aggregated* in the IT strategic balanced scorecard. This, in turn is fed into and evaluated against the business objectives. In this way, the service (and value) delivered by IT is directly measured against the objectives of the overall business. Further, on an annual basis, the IT strategic BSC is reviewed by business and IT management and the result is fed back into the next annual planning cycle. This planning cycle defines what the business needs are and what IT must do to accomplish those needs.

For example, from the IT service desk scorecard (i.e., a unit scorecard, which is situated in the operational services scorecard group), metrics such as average speed of answer, overall resolution rate at initial call, and call abandonment rate (all three

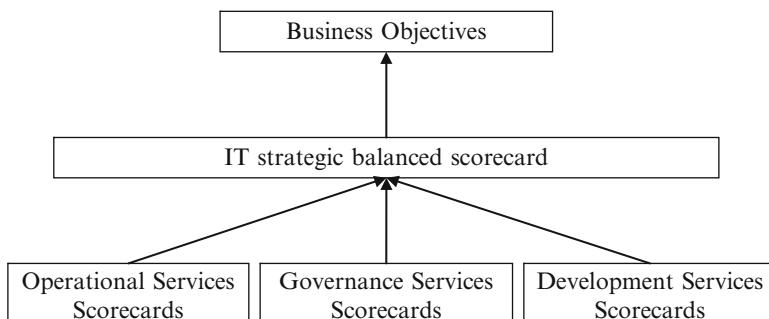


Fig. 4.17 Cascade of scorecards

customer orientation metrics) are *rolled-up* to service level performance metrics in the IT strategic balanced scorecard. Other metrics of this unit scorecard such as expense management (corporate contribution perspective), client satisfaction (customer orientation perspective), process maturity of incident management (operational excellence perspective), and staff turnover (future orientation perspective), will *aggregate* as part of the IT strategic scorecard. The overall view of the IT strategic balanced scorecard is then fed into and evaluated against the defined business objectives.

The second way to demonstrate business value is situated within the IT strategic balanced scorecard. The cause-and-effect relationships between performance drivers and outcome measures of the four quadrants are established as indicated in Fig. 4.18. These connections help to understand how the contribution of IT towards the business will be realized: building the foundation for delivery and continuous learning & growth (future orientation perspective) is an enabler for carrying out the roles of the IT division's mission (operational excellence perspective) that is in turn an enabler for measuring up to business expectations (customer expectations perspective) that eventually must lead to ensuring effective IT governance (corporate contribution perspective). The construction of cause-and-effect relationships is a critical issue in the further development of the IT strategic BSC. These relationships have not yet been explicitly defined although they are implicit in the existing scorecard. For example, the *Professional development days per staff member* measure can be identified as a performance driver for the outcome measures *Development process performance*.

The Corporate contribution perspective of Fig. 4.18 is an enabler (performance driver) of the (generic) business objectives of the financial Group with its specific measures such as *Business/IT alignment*, *Value delivery*, *Cost management*, *Risk management*, and *Intercompany synergy achievement*. The CIO and its executive management are aware that an explicit articulation of these relationships has to be done and that it may help to improve the IT strategic BSC and its link with the business objectives, later on with the implementation of a Business BSC.

Assignment Box 4.2: Cause-and-Effect Relationship

A major point in developing an IT Balanced Scorecard is identifying the cause-and-effect relationships across the whole scorecard. In the case study, these relationships are not described. Identify what you think are outcome measures and what their corresponding performance drivers are

Assignment Box 4.3: Cascade of Scorecards

At the case company there are, besides the IT strategic balanced scorecard, also scorecards implemented at unit level. The measures of these unit scorecards are rolled-up or aggregated in the IT strategic balanced scorecard. Develop a generic scorecard for the IT development department.

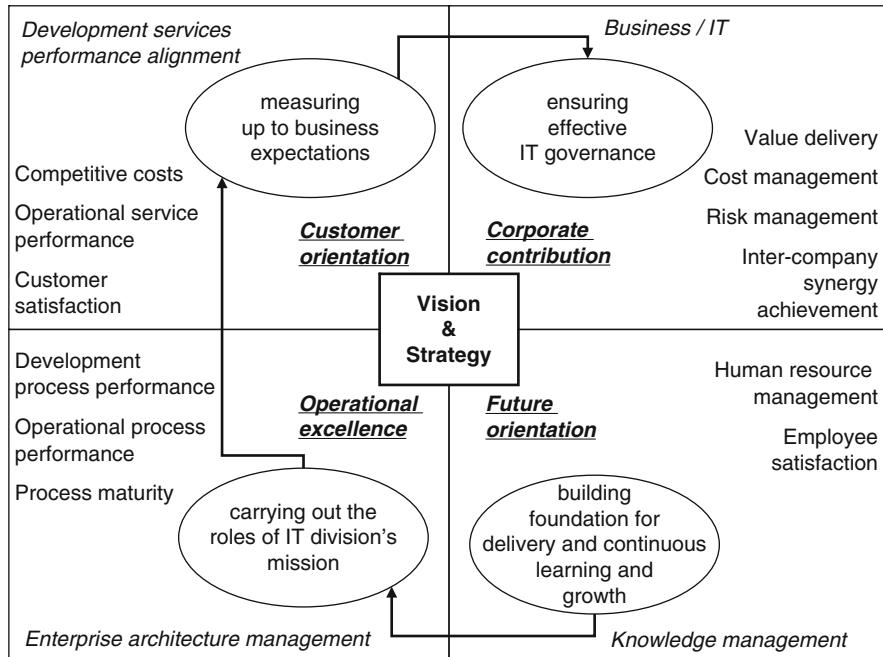


Fig. 4.18 IT strategic scorecard objectives and cause-and-effect

Summary

Investments in IT are growing extensively, and business managers often worry that the benefits of IT investments might not be as high as expected. The same worry accounts for the perceived ever-increasing total cost of the IT department, without clear evidence of the value derived from it. This phenomenon is called the “IT black hole”: large sums go in, but no returns (seem to) come out. In this chapter, we discussed the use of the business case, throughout the life cycle of an investment, as an important instrument to realize benefits out of IT-enabled investments. Also, the IT balanced scorecard is presented as an approach to measure and manage both financial and nonfinancial benefits coming out of IT-enabled investments and departments.

Study Questions

1. Describe the concept of the IT black hole. Explain how it relates to the “IT doesn’t matter” article discussed in Chap. 1.
2. Explain why and how the business case could be used in the context of an IT-enabled investment.

3. Explain how the balanced scorecard can be applied to the IT function.
4. How can you leverage the IT BSC as a management and alignment instrument?
5. Explain and illustrate the difference between outcome measures and performance drivers.
6. Explain the concept of the “cascade of scorecards.”
7. Explain the aggregating and rolling up mechanism of metrics and indicate which typical IT metrics you think should appear on the business balanced scorecard.

Acknowledgment For this chapter, we want to explicitly acknowledge Kim Maes, who worked on the concepts of the business case in the context of his Ph.D. project. Parts of the research we worked on together are included in this chapter.

References

- Al-Mudimigh, A., Zairi, M., & Al-Mashari, M. (2001). ERP software implementation: An integrative framework. *European Journal of Information Systems*, 10(4), 216–226.
- Altinkemer, K., Ozcelik, Y., & Ozdemir, Z. (2011). Productivity and performance effects of business process reengineering: A firm-level analysis. *Journal of Management Information Systems*, 27(4), 129–162.
- Ashurst, C., Doherty, N., & Peppard, J. (2008). Improving the impact of IT development projects: The benefits realization capability model. *European Journal of Information Systems*, 17(4), 352–370.
- Beatty, R., & Williams, C. (2006). ERP II: Best practices for successfully implementing an ERP upgrade. *Communications of the ACM*, 49(3), 105–109.
- Brown, D. H., & Lockett, N. (2004). Potential of critical e-applications for engaging SMEs in e-business: a provider perspective. *European Journal of Information Systems*, 13(1), 21–34.
- Davenport, T. H., Harris, J., & Shapiro, J. (2010). Competing on talent analytics. *Harvard Business Review*, 88(10), 52–58.
- Flynn, D., Pan, G., Keil, M., & Mähring, M. (2009). De-escalating IT projects: the DMM model. *Communications of the ACM*, 52(10), 131–134.
- Fonstad, N., & Robertson, D. (2006). Transforming a company, project by project: The IT engagement model. *MIS Quarterly Executive*, 5(1), 1–14.
- Franken, A., Edwards, C., & Lambert, R. (2009). Executing strategic change: Understanding the critical management elements that lead to success. *California Management Review*, 51(3), 49–73.
- Goldschmidt, P. (2005). HIT and MIS: Implications of health information technology and medical information systems. *Communications of the ACM*, 48(10), 68–74.
- ISACA. (2008) Enterprise value: Governance of IT investments: The business case. www.isaca.org.
- ITGI. (2000). *CobiT: Governance, control and audit for information and related technology*. Rolling Meadows, IL: IT Governance Institute.
- Jeffrey, M., & Leliveld, I. (2004). Best practices in IT portfolio. *MIT Sloan Management Review*, 45(3), 41–49.
- Kaplan, R., & Norton, D. (1996). *The balanced scorecard: Translating vision into action*. Boston: Harvard Business School Press.
- Krell, K., & Matook, S. (2009). Competitive advantage from mandatory investments: An empirical study of Australian firms. *The Journal of Strategic Information Systems*, 18(1), 31–45.
- Lacovou, C., & Dexter, A. (2004). Turning around runaway information technology projects. *California Management Review*, 46(4), 68–88.
- Law, C., & Ngai, E. (2007). ERP systems adoption: An exploratory study of the organizational factors and impacts of ERP success. *Information & Management*, 44(4), 418–432.

- Luna-Reyes, L., Zhang, J., Gil-García, J., & Cresswell, A. (2005). Information systems development as emergent socio-technical change: A practice approach. *European Journal of Information Systems*, 14(1), 93–105.
- Maes, K., De Haes, S., & Van Grembergen, W. (2014). Investigating a process approach on business cases: An exploratory case study at Barco. *International Journal of IT/Business Alignment and Governance*, 4, 2.
- Maes Kim, De Haes Steven, Van Grembergen Wim. Using a business case throughout an investment: An exploratory case study on a business case process. *Proceedings of Americas Conference of Information Systems (AMCIS)* Chicago, 2013
- Matthews, H. (2004). Thinking outside “the Box”: Designing a packaging take-back system. *California Management Review*, 46(2), 105–119.
- Post, B. (1992). A business case framework for group support technology. *Journal of Management Information Systems*, 9(3), 7–26.
- Powell, P. (1993). Causality in the alignment of information technology and business strategy. *The Journal of Strategic Information Systems*, 2(4), 320–334.
- Sherif, K., & Vinze, A. (2002). Domain engineering for developing software repositories: A case study. *Decision Support Systems*, 33(1), 55–69.
- Smith, H., McKeen, J., Cranston, C., & Benson, M. (2010). Investment spend optimization: A new approach to IT investment at BMO financial group. *MIS Quarterly Executive*, 9(2), 65–81.
- Taudes, A., Feurstein, M., & Mild, A. (2000). Options analysis of software platform decisions: A case study. *MIS Quarterly*, 24(2), 227–243.
- Van Der Zee, J. T. M., & De Jong, B. (1999). Alignment is not enough: Integrating business and information technology management with the balanced business scorecard. *Journal of Management Information Systems*, 16(2), 137–156.
- Van Grembergen, W., & De Haes, S. (2005a). Measuring and demonstrating the value of IT, in IT Governance Domain Practices and Competencies (Series of IT Governance Institute)
- Van Grembergen, W., & De Haes, S. (2005b). Measuring and improving IT governance through the balanced scorecard. *Information Systems Control Journal*, 2.
- Van Grembergen, W., & Van Bruggen, R. (1997). *Measuring and improving corporate Information Technology through the balanced scorecard technique*. In *Proceedings of the European Conference on the Evaluation of Information Technology*. Delft, The Netherlands
- Van Grembergen, W., Saull, R., & De Haes, S. (2003). Linking the IT balanced scorecard to the business objectives at a major Canadian financial group. *Journal for Information Technology Cases and Applications (JITCA)*, 5(1).
- Ward, J., Daniel, E., & Peppard, J. (2008). Building better business cases for IT investments. *MIS Quarterly Executive*, 7(1), 1–15.

Chapter 5

COBIT as a Framework for Enterprise Governance of IT

Abstract Enterprises are increasingly making tangible and intangible investments in improving enterprise governance of IT. In support of this, enterprises are drawing upon the practical relevance of generally accepted good-practice frameworks such as COBIT. COBIT (Control Objectives for Information and Related Technologies), now in its fifth edition, is an internationally recognized industry framework that describes a set of good practices for the board, executive management, and operational business and IT managers. It sets out a set of controls over information technology, and organizes them around a logical framework of IT-related processes and enablers.

5.1 COBIT History

COBIT is developed by ISACA (Information Systems Audit and Control Association), an international professional membership association for IT professionals and IT auditors counting more than 100,000 members worldwide. COBIT initially originated in the mid-90s out of the (financial) audit community. Those audit professionals were confronted more and more with automated environments. To guide their work in these IT-related environments, COBIT was initially developed as a framework for executing IT audit assignments, built around a comprehensive set of Control Objectives for IT processes. Building on this IT auditing basis, the COBIT framework was developed further becoming a broader IT management framework, within 2000 the addition of “Management Guidelines” in COBIT version 3, including metrics, critical success factors, and maturity models for IT processes. In 2005 again a new release was issued, COBIT 4, containing several new management and governance concepts, such as (1) the alignment of business and IT goals and their relationship with supporting IT processes, (2) roles and responsibilities within IT processes, and (3) the interrelationship between IT processes. With these extensions COBIT wanted to continue to establish itself as a generally accepted framework for IT governance (Van Grembergen & De Haes, 2009).

Fig. 5.1 COBIT, VALIT, and RISKIT as frameworks for enterprise governance of IT



In the shift from IT governance to enterprise governance of IT, as discussed in Chaps. 1 and 2, ISACA complemented its IT governance best practices framework COBIT, focusing on IT processes and responsibilities, with the Val IT and RISKIT framework (ISACA, 2008, 2009), addressing the IT-related business processes and responsibilities in value creation (VALIT) and risk management (RISKIT). In the field, COBIT, RISKIT, and VALIT are considered to be strong reference frameworks guiding managers to implement enterprise governance of IT in their organization, as visualized in Fig. 5.1 (Van Grembergen & De Haes, 2009).

In April 2012, the latest version COBIT 5 was released, referencing the concept of enterprise governance of IT on its cover (ISACA, 2012). According to the ISACA website, “COBIT 5 provides a comprehensive framework that assists enterprises to achieve their objectives for the governance and management of enterprise IT. ... COBIT 5 enables IT to be governed and managed in a holistic manner for the whole enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders” (ISACA, 2012). COBIT 5 will integrate all knowledge previously dispersed over the three important ISACA frameworks COBIT, VALIT, and RISKIT, as such becoming a “one-stop-shop” to enter ISACA’s body of knowledge.

5.2 COBIT 5 Principles

The COBIT 5 manuals state that the framework is built around five core principles, as visualized in Fig. 5.2. Each of those principles are discussed in this section and related to concepts and insights from general and IT literature.

5.2.1 *Meeting Stakeholder Needs: Strategic Business/IT Alignment*

According to ISACA, Principle 1 (Meeting Stakeholder Needs) implies that COBIT 5 provides all the required processes and other enablers to support business value creation through the use of IT, as such meeting all stakeholder needs. This principle

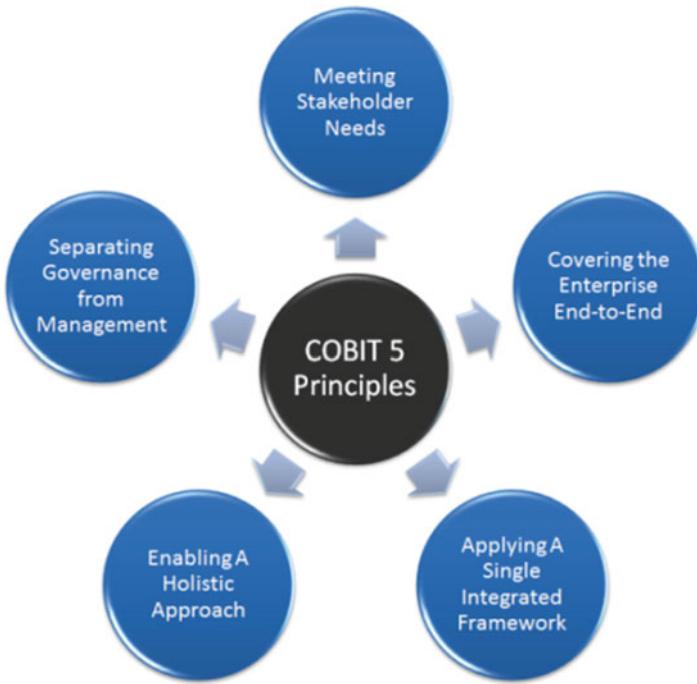


Fig. 5.2 COBIT 5 principles. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

closely links to the “Strategic Alignment” discussion as initiated by Henderson and Venkatraman in 1993 (see also Chap. 3).

The idea behind strategic alignment is very comprehensive and has been present in all COBIT documentation since the first release. However, the challenge is how organizations can achieve this ultimate objective. To answer this question, a series of research steps has been set up by the development team in order to provide guidance in understanding how enterprise goals drive IT-related goals and vice versa (Van Grembergen et al. 2007). Throughout these research projects, and based on many in-depth interviews in different sectors and expert team interrogations, a generic list of enterprise goals, IT-related goals and its interrelationship was established, as shown in Fig. 5.3 (p=primary link; s=secondary link). This cascade now constitutes the core entry point of COBIT 5, implying that organizations should always start with analyzing their alignment situation through defining and linking enterprise goals and IT-related goals (De Haes & Van Grembergen, 2010; Van Grembergen et al., 2008).

Important to mention is that COBIT 5 uses the word “Enterprise Goals” instead of “Business Goals” as referenced in COBIT 4. With this shift, COBIT 5 wants to explicitly include both profit and nonprofit (government) types of enterprises. Also, COBIT 5 talks about “IT-related” goals and not about “IT goals” anymore as in COBIT 4. The reason for that is also explained in the next “COBIT principle,” addressing the conviction that both business and IT people have “IT-related” responsibilities in realizing value out of IT.

As an illustration of this cascade, Fig. 5.3 shows that the enterprise goal of “External compliance with laws and regulation” requires primary focus (P) on the IT-related goals of “security of information and processing infrastructure.” In the further documentation of COBIT 5, the importance of this IT-related goal will in turn lead to (see Fig. 5.4) the primary focus on some of the identified enablers for governance and management of enterprise IT, such as the COBIT 5 processes “Manage Risks,” “Manage Security,” and “Manage Changes.”

5.2.2 *Meeting Stakeholder Needs: The Balanced Scorecard*

To verify whether stakeholder needs are indeed being met, a sound measurement process needs to be established. Traditional performance methods such as return on investment (ROI) capture the financial worth of IT projects and systems, but reflect only a limited (tangible) part of the value that can be delivered by IT (Van Grembergen & De Haes, 2009).

To enable a broader measurement process, the developers of COBIT have built on the concepts of the IT-balanced scorecard as developed by Kaplan and Norton (1996) and Van Grembergen et al. (2003). As shown in Fig. 5.3, all enterprise goals and IT-related goals are grouped in the balanced scorecard perspectives. COBIT also provides samples of outcome metrics to measure each of those goals and to really build a scorecard for IT-related activities. Figure 5.5 provides some examples of such metrics for the “customer perspective” of the enterprise goals and the IT-related goals.

Moreover, COBIT 5 provides outcome measures at the level of the 37 detailed COBIT 5 processes. An example is shown in Fig. 5.6 for the process of Managing Security, providing specific process goals and related metrics. Consolidating all these metrics, at enterprise level, IT-related level, and COBIT processes level, enables organization to build a comprehensive scorecard for the entire IT-related environment, as an instrument to verify whether stakeholder needs are being met.

5.2.3 *Covering the Enterprise End-to-End: IT Savviness*

The next principle (Covering the Enterprise End-to-End) articulates that COBIT 5 does not only focus on the “IT function,” but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise. This statement related to the work of Weill and Ross (2009) on IT Savviness, concluding that business people should take up responsibility in managing their IT-related assets. Their work clarifies the need for the business to take ownership of, and be accountable for, governing the use of IT in creating value from IT-enabled business investments.

		Enterprise Goals															Learning & Growth	
		Internal																
IT Related Goals	1 Alignment of IT and business strategy	S	S	P	P	S	P	S	P	S	P	S	P	S	S	S	P	
	2 IT compliance with external laws and regulations	P	S	S	P	S	P	S	P	S	P	S	P	S	S	S		
	3 Commitment of executive management for taking IT decisions	S	P	S	P	S	P	S	P	S	P	S	P	S	S	S	P	
	4 Managed IT related business risks	S	P	S	P	S	P	S	P	S	P	S	P	S	S	S		
	5 Realized benefits from IT enabled investments and services portfolio	S	S	P	P	S	P	S	P	S	P	S	P	S	S	S	P	
	6 Transparency of IT costs, benefits and risk	P	P	S	P	S	P	S	P	S	P	S	P	S	S	S		
	7 IT services in line with business requirements	S	P	S	P	S	P	S	P	S	P	S	P	S	S	S	P	
	8 Adequate use of applications, information and technology solutions	S	S	P	P	S	P	S	P	S	P	S	P	S	S	S		
	9 IT agility	S	S	P	P	S	P	S	P	S	P	S	P	S	S	S	S	
	10 Security of information and processing infrastructure	P	P	S	P	S	P	S	P	S	P	S	P	S	S	S		
	11 Optimisation of IT infrastructure, resources and capabilities	S	S	P	P	S	P	S	P	S	P	S	P	S	S	S	S	
	12 Integration of applications and technology into business processes	S	S	P	P	S	P	S	P	S	P	S	P	S	S	S		
	13 Delivery of programmes on time, on budget and meeting quality standards	S	S	P	P	S	P	S	P	S	P	S	P	S	S	S	S	
	14 Availability of reliable and useful information	S	S	P	P	S	P	S	P	S	P	S	P	S	S	S		
	15 IT compliance with internal policies	P	S	S	P	S	P	S	P	S	P	S	P	S	S	S	P	
	16 Competent and motivated IT people	P	S	S	P	S	P	S	P	S	P	S	P	S	S	S		
	17 Knowledge, expertise and initiatives for business innovation	S	S	P	P	S	P	S	P	S	P	S	P	S	S	S	P	

Fig. 5.3 Enterprise goals and IT-related goals. Source: ISACA, COBIT 5, www.isaca.org/COBIT

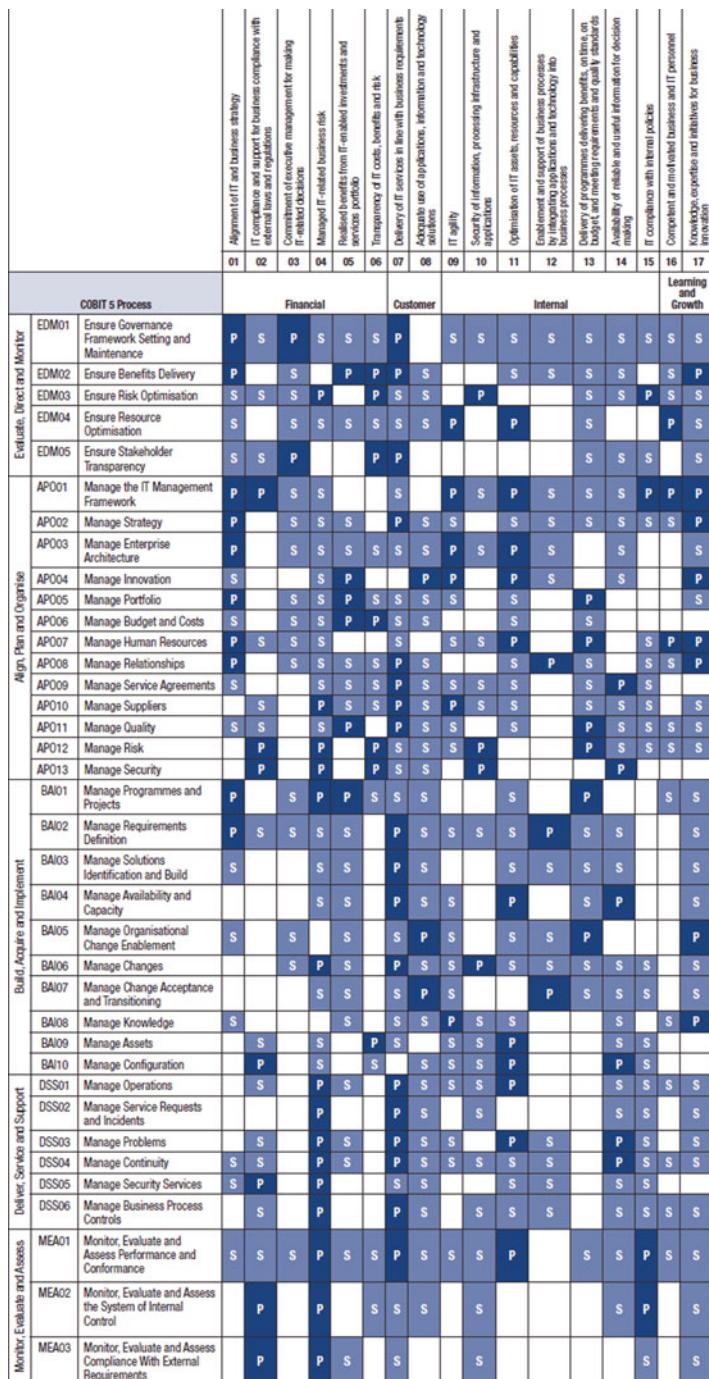


Fig. 5.4 Cascade of IT-related goals and COBIT 5 processes. Source: ISACA, COBIT 5, www.isaca.org/COBIT

BSC Dimension	Enterprise Goal	Metric
Customer	6. Customer-oriented service culture	<ul style="list-style-type: none"> Number of customer service disruptions due to IT service-related incidents (reliability) Percent of business stakeholders satisfied that customer service delivery meets agreed-on levels Number of customer complaints Trend of customer satisfaction survey results
	7. Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets
	8. Agile responses to a changing business environment	<ul style="list-style-type: none"> Level of board satisfaction with enterprise responsiveness to new requirements Number of critical products and services supported by up-to-date business processes Average time to turn strategic enterprise objectives into an agreed-on and approved initiative
	9. Information-based strategic decision making	<ul style="list-style-type: none"> Degree of board and executive management satisfaction with decision making Number of incidents caused by incorrect business decisions based on inaccurate information Time to provide supporting information to enable effective business decisions
	10. Optimisation of service delivery costs	<ul style="list-style-type: none"> Frequency of service delivery cost optimisation assessments Trend of cost assessment vs. service level results Satisfaction levels of board and executive management with service delivery costs

BSC Dimension	IT-related Goal	Metric
Customer	07 Delivery of IT services in line with business requirements	<ul style="list-style-type: none"> Number of business disruptions due to IT service incidents Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels Percent of users satisfied with the quality of IT service delivery
	08 Adequate use of applications, information and technology solutions	<ul style="list-style-type: none"> Percent of business process owners satisfied with supporting IT products and services Level of business user understanding of how technology solutions support their processes Satisfaction level of business users with training and user manuals Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions

Fig. 5.5 Balanced scorecard metrics for enterprise goals and IT-related goals. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

Process Goals and Metrics	
Process Goal	Related Metrics
1. A system is in place that considers and effectively addresses enterprise information security requirements.	<ul style="list-style-type: none"> Number of key security roles clearly defined Number of security related incidents
2. A security plan has been established, accepted and communicated throughout the enterprise.	<ul style="list-style-type: none"> Level of stakeholder satisfaction with the security plan throughout the enterprise Number of security solutions deviating from the plan Number of security solutions deviating from the enterprise architecture
3. Information security solutions are implemented and operated consistently throughout the enterprise.	<ul style="list-style-type: none"> Number of services with confirmed alignment to the security plan Number of security incidents caused by non-adherence to the security plan Number of solutions developed with confirmed alignment to the security plan

Fig. 5.6 Balanced scorecard metrics for the security process. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

This implies a crucial shift in the minds of the business and IT, moving away from managing IT as a “cost” toward managing IT as an “asset” to create business value. As Weill and Ross describe in their 2009 “IT Savvy” book: “If senior managers do not accept accountability for IT, the company will inevitably throw its IT money to multiple tactical initiatives with no clear impact on the organizational capabilities. IT becomes a liability instead of a strategic asset.”

Related to this discussion, COBIT 5 talks about “Covering the Enterprise End-to-End.” COBIT 5 does cover both IT processes and IT-related business processes. As a demonstration of this, COBIT 5 provides RACI charts (Responsible, Accountable,

Key Management Practice		Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP009.01	Identify IT services.	C	R	R	R	C	I							I	I	R	I	C	C	C	A	I	I				
AP009.02	Catalogue IT-enabled services.			I	I		I							I	I	R	I	C	C	C	A	I	I				
AP009.03	Define and prepare service agreements.			R	C		C	C						C	C	R		C	R	R	A	C	C				
AP009.04	Monitor and report service levels.	I	I	I	R					C					I		I	I	I	A							
AP009.05	Review service agreements and contracts.			A	C		C	C						C	C	R		C	R	R	R	C	C	I			

Fig. 5.7 End-to-end responsibility in managing service agreements. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

Consulted, Informed) in which both business roles and IT roles are included. To illustrate this, an example RACI chart for the process “Manage Service Agreements” is shown in Fig. 5.7. This RACI chart indicates that for the service level agreements (SLA) process both business and IT functions have accountabilities and responsibilities.

5.2.4 Applying a Single, Integrated Framework: COBIT/RISKIT/VALIT

Principle 3 (Applying a Single, Integrated Framework) explains that COBIT 5 aligns with other relevant standards and frameworks at a high level, and thus can serve as the overarching framework for governance and management of enterprise IT. COBIT 5 becomes an overall integration, or one-stop-shop, of all previous ISACA-related materials as published COBIT 4, VALIT, and RISKIT (ISACA, 2007, 2008, 2009).

In this overarching approach, COBIT amongst others identifies 37 processes spread over a governance and a management domain, as visualized in Fig. 5.8. The five governance processes are the board’s responsibilities in IT, covering the setting of the governance framework, responsibilities in terms of value (e.g., investment criteria), risks (e.g., risk appetite) and resources (e.g., resource optimization), and providing transparency regarding IT to the stakeholders. In the management area, four subdomains are defined: Align, Plan, Organize (APO), Build, Acquire, and Implement (BAI), Deliver, Service, and Support (DSS), and Monitor, Evaluate, and Assess (MEA). The domain APO concerns the identification of how IT can best

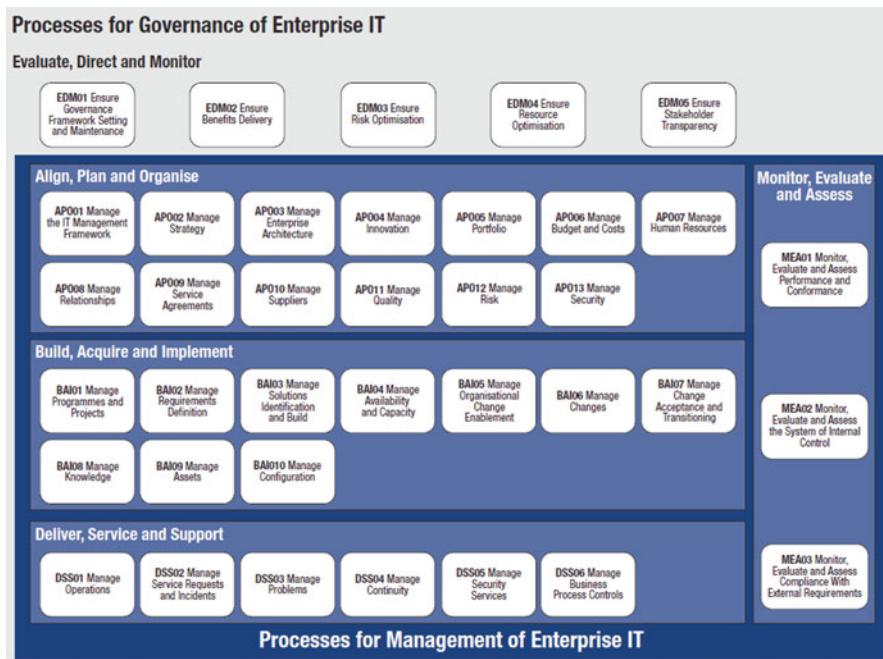


Fig. 5.8 COBIT 5 processes. Source: ISACA, COBIT 5, www.isaca.org/COBIT

contribute to the achievement of the business objectives. A management framework is required, and specific processes related to the IT strategy and tactics, enterprise architecture, innovation and portfolio management. Other important processes in this domain address the management of budgets and costs, human resources, relationships, service agreements, suppliers, quality, risk, and security. The domain BAI concretizes the IT strategy through identifying in detail the requirements for IT and managing programme and projects. This domain further talks about managing capacity, organizational change, IT changes, acceptance and transitioning, knowledge, assets, and configurations. The domain Delivery and Support refers to the actual delivery of required services. It contains processes around managing operations, service requests and incidents, problems, continuity, security services, and business process controls. The fourth management domain, MEA, includes those processes that are responsible for the quality assessment in compliance with the control requirements for all previously mentioned processes. It addresses performance management, monitoring of internal control and regulatory compliance (ISACA, 2012).

As can be seen in previous figure, COBIT 5 offers a very broad view on the knowledge area of enterprise governance and management of IT. In its development, COBIT always tried to align and integrate with other important international frameworks. At a high level, it could be said that COBIT provides a very complete and broad overview of “what” needs to be done in enterprise governance and

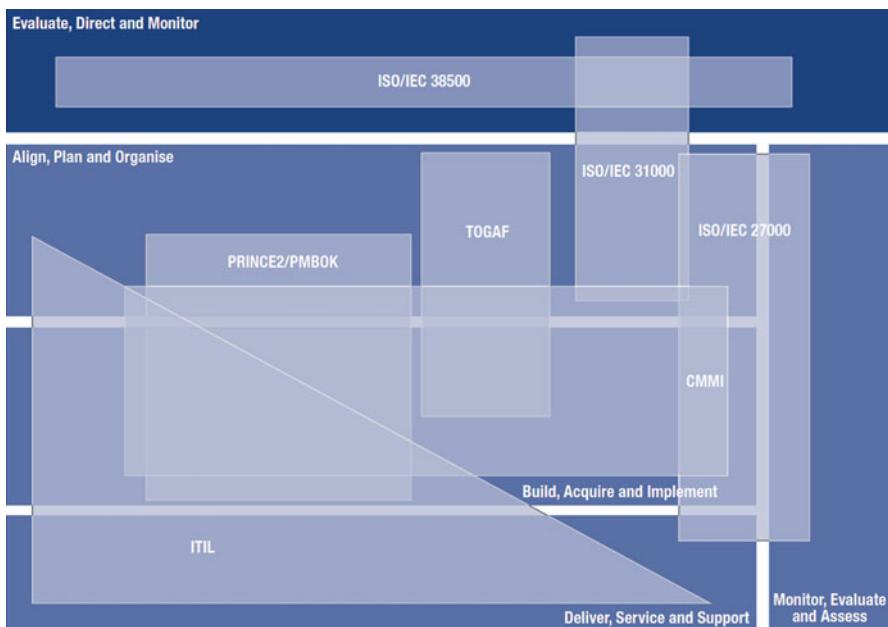


Fig. 5.9 COBIT related to other standards. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

management of IT. More detailed guidance can then often be found in related standards and practices, as can be seen in Fig. 5.9. For example, the delivery, service, and support processes are very close to what is discussed in ITIL, the “BAI1—Manage programmes and project” process is related to Prince 2/PMBOK, the APO2 process on enterprise architecture related to TOGAF, etc.

5.2.5 Applying a Single Integrated Framework: IT Savviness

Comparing the set of processes (see Fig. 5.8) with previous versions of COBIT clearly demonstrates the extension towards business roles and responsibilities in governing and managing IT. Again, this extension fully aligns with the requirement of business people taking up accountable in managing IT, as put forward in the IT savviness discussion.

For example, newly inserted processes that address specific business roles are APO3: Manage Enterprise Architecture, APO4: Manage Innovation, and BAI05: Manage Organizational Change. In this context, specific attention goes to “DS06: Manage Business Process Controls.” This process was removed out of the previous version of COBIT, as the previous version focused more on the responsibilities of the IT department. Managing business process controls (application controls) was considered to be out of scope, being a prime accountability of the business. However, COBIT 5 aims to include both business and IT responsibilities in managing and governing IT. For that reason, the process on business process controls was re-included in COBIT 5.

As a side note, it should also be mentioned that there are much less processes in the “Deliver, Service, and Support” domain (6) as compared to the number of processes in the “Deliver and Support” domain of previous COBIT version (13). Many of these processes are moved to a higher domain. A typical example is the shift of Manage Service Agreements to APO, argumented by the recent evolution of the externalization of IT operations through outsourcing and cloud computing.

5.2.6 Enabling a Holistic Approach: Organizational Systems

The fourth principle (Enabling a Holistic Approach) explains that efficient and effective implementation of governance and management of enterprise IT requires a holistic approach, taking into account several interacting components, such as Processes, Structures, and People.

This implementation challenge is related to what is described in strategic management literature as the need for an organizational system, i.e., “the way a firm gets its people to work together to carry out the business” (De Wit & Meyer, 2005). Such organizational system requires the definition and application, in a holistic whole, of structures (e.g., organizational units and functions) and processes (to ensure tasks are coordinated and integrated), and attention to people and relational aspects (e.g., culture, values, joint beliefs, etc.).

Peterson (2004) and De Haes and Van Grembergen (2008, 2009), have applied this organizational system theory to the discussion of enterprise governance of IT. These authors conclude that organizations can and are deploying enterprise governance of IT by using a holistic mixture of various structures, processes, and relational mechanisms. Enterprise governance of IT structures include organizational units and roles responsible for making IT decisions and for enabling contacts between business and IT management decision-making functions (e.g., IT steering committee). This can be seen as a form of blueprint for how the governance framework will be structurally organized. Enterprise governance of IT processes refers to the formalization and institutionalization of strategic IT decision-making and IT monitoring procedures, to ensure that daily behaviors are consistent with policies and provide input back to decisions (e.g., IT-balanced scorecard). The relational mechanisms are ultimately about the active participation of, and collaborative relationship among, corporate executives, IT management, and business management, and include mechanisms such as announcements, advocates, and education efforts.

COBIT 5 builds on these insights and talks about “Enablers” in its framework. Enablers are defined as factors that, individually and collectively, influence whether something will work in this case, governance and management over enterprise IT. The COBIT 5 framework describes seven categories of enablers (see Fig. 5.10), of which the “processes,” “organizational structures,” “culture, behavior, and ethics,” and “people, skills, and competencies” are closely related to the three elements proposed in the organizational systems concept.

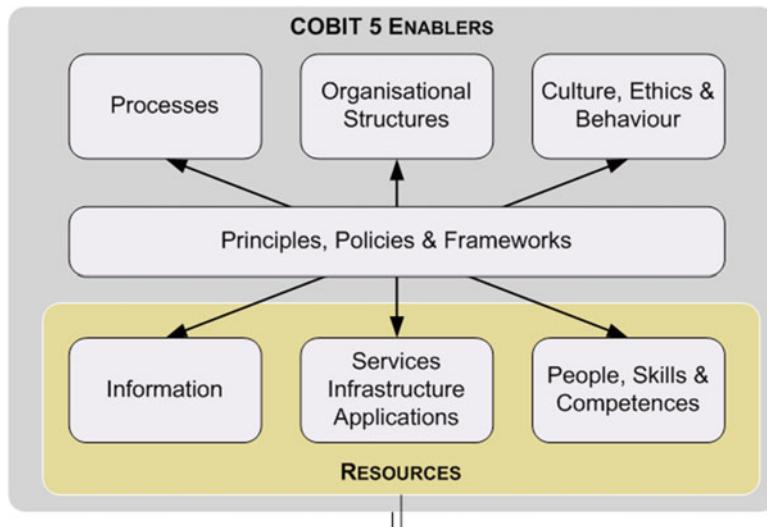


Fig. 5.10 Organizational systems of enablers. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

5.2.7 *Separating Governance from Management: ISO/IEC 38500*

Principle 5 finally (Separating Governance from Management) is about the distinction COBIT 5 makes between governance and management, which, as discussed before, heavily builds on the position put forward by ISO/IEC 38500 (ISACA, 2012). In COBIT 5, ISACA states for the first time that these IT governance and IT management processes encompass different types of activities. The governance processes are organized following the EDM model (“Evaluate—Direct—Monitor”), as proposed by the ISO/IEC 38500 standard on Corporate Governance of IT (ISO/IEC, 2008). IT governance processes ensure that enterprise objectives are achieved by evaluating stakeholder needs, directing and delegating decision roles, responsibilities, and processes, and monitoring performance, compliance and progress against plans. In enterprises, IT governance should be the accountability of the board of directors under the leadership of the chairperson. Based on these governance activities, business and IT management plans, builds, runs, and monitors activities (a COBIT translation of Deming’s PDCA circle Plan, Do, Check, Act) in alignment with the direction set by the governance body to achieve the enterprise objectives (ISACA, 2012). This all is in line with the (adapted) definition as formulated in a preceding paragraph: IT governance is the Board’s accountability and the execution is executive’s responsibility (Van Grembergen & De Haes, 2009).

5.3 COBIT 5 Enabling Processes and Domains

As discussed in previous section, COBIT 5 proposes seven enablers that are required to adopt enterprise governance and management of IT. This section discusses one of the most important enablers in detail, more specifically the process enabler, by developing one specific process example at a more granular level.

The way the COBIT 5 processes are visualized is very close the COBIT 4 look and feel, with elements like RACI charts, inputs/outputs, goals and metrics, etc. This continuity in structure and look and feel was done to make the transition between COBIT 4 and COBIT 5 as easy as possible. Important to mention is that COBIT 5 does not have any “maturity models” anymore. Instead, a new assessment programme was developed based on the ISO 15504 standard. This will be discussed in a separate section.

The following section illustrates the material that COBIT 5 provides for the process of “Manage Service Requests & Incidents” (DSS 2).

5.3.1 *Process Description and Purpose*

For each COBIT 5 process, a short general description is provided which summarizes the core content of the process. The process “Manage service requests and incidents” is defined as follows: “Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfill user requests; and record, investigate, diagnose, escalate, and resolve incidents.”

This process description is then followed by some statements around the general purpose of the process (Fig. 5.11). Or in other words, it describes the main reasons why an organization should consider to implement this process. For the process under review, the purpose statement is defined as: “Achieve increased productivity and minimize disruptions through quick resolution of use queries and incidents.”

5.3.2 *Goals and Metrics*

In the next section, the process description and purpose are translated into a more detailed set of goals and metrics at different levels (Fig. 5.12). Fully aligned with the concepts of the balanced scorecard (see related chapter in this book), these metrics can be categorized as “outcome measures” for each of the postulated goals. As an example for the process DSS2, the following goal is formulated “incidents are resolved according to the agreed service levels.” A related outcome measure identified is stated as followed: “percent of incidents resolved with an agreed-upon/acceptable period of time.”

DSS02	Manage Service Requests and Incidents	Area: Management Domain: Deliver, Service and Support
-------	---------------------------------------	--

Process Description

Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.

Process Purpose Statement

Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.

Fig. 5.11 Process description and purpose statement. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

Process Goals and Metrics	
Process Goal	Related Metrics
1 IT-related services are available for use.	Mean time between incidents per IT-enabled service Number and percent incidents causing disruption to business-critical processes
2 Incidents are resolved according to the agreed service levels.	Percent incidents resolved within an agreed-upon/acceptable period of time
3 Service requests are dealt with according to agreed service levels and to the satisfaction of users.	Level of user satisfaction with service request fulfilment Mean elapsed time for handling each type of service request

Fig. 5.12 Process goals and metrics. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

The process supports the achievement of a set of primary IT-related goals:	
IT related Goal	Related Metrics
04 Managed IT-related business risks	Percent critical business processes, IT services and IT-enabled business programmes covered by risk assessment Number of significant IT-related incidents that were not identified in risk assessment Percent enterprise risk assessments including IT-related risks Update frequency of risk profile
07 Delivery of IT services in line with business requirements	Number of business disruptions due to IT service incidents Percent business stakeholders satisfied that IT service delivery meets agreed-upon service levels Percent users satisfied with quality of IT service delivery

Fig. 5.13 IT-related goals and metrics. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

Next to the process goals and metrics, also goals and metrics at a higher level are defined. These goals are called “IT-related goals,” and the assumption is that if process goals are achieved, that this will contribute to the better achievement of the IT-related goals (Fig. 5.13). This implies that the process goals and metrics become “performance drivers” for the IT-related goals and corresponding outcome measure at their specific higher level. An example: if the process goals 2 (“incidents are resolved according to the agreed service levels”) is realized, the likelihood is high that the higher-level IT-related goals of “delivery of IT services in line with business requirements” is impacted positively. The latter goal could be measured through the outcome measure of “number of business disruptions due to IT service incidents.”

COBIT 5 also identifies, next to the process and IT-related goals and metrics, also goals and metrics at enterprise level. As such, a cascade can be developed describing how process goals drive the achievement of IT-related goals, which in

DSS02 RACI Chart																										
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS02.01 Define incident and service request classification schemes.					C				I I								A C R R		R C C C							
DSS02.02 Record, classify and prioritise requests and incidents.					I				I I									A	R			I				
DSS02.03 Verify, approve and fulfil service requests.					R				I I								I R R		A							
DSS02.04 Investigate, diagnose and allocate incidents.					R				I I					I I I			C R		A C							
DSS02.05 Resolve and recover from incidents.					I				I I					C C I			R R		A R			C				
DSS02.06 Close service requests and incidents.					I				I I					I I I			I A		I R		I					
DSS02.07 Track status and produce reports.					I				I I					I I I			I A		R I							

Fig. 5.14 RACI chart. Source: ISACA, COBIT 5, www.isaca.org/COBIT

turn drive the achievement of enterprise goals. This material provides a wealth of information to build a balanced scorecard for different IT-related matters in organizations.

5.3.3 RACI Chart

Each COBIT process is decomposed into activities and roles and responsibilities in the format of a RACI chart (R=responsible, A=accountable, C=consulted, I=Informed) (Fig. 5.14). In the RACI chart, the left column identifies a number of key management practices and for each practice, an indication is given on who is responsible, accountable, consulted, and informed. In the example process under review, DSS 2 is decomposed into seven management practices, including “define incident and service request classification schemes” and “record, classify, and prioritize requests and incidents.”

The roles that are mentioned in the RACI chart in the top row are also defined in the COBIT 5 manuals (Fig. 5.15). The RACI chart includes both “business-” oriented roles (e.g., business sponsor, CEO) and IT-oriented roles (e.g., CIO, Head IT operations). For the more operational oriented DSS 2 process under review, the RACI chart shows that most of the “A” and “R” are expected to be organized within the IT department.

Role/Structure	Definition/Description
Board	The group of the most senior executives and/or non-executive directors of the enterprise who are accountable for the governance of the enterprise and have overall control of its resources
CEO	The highest-ranking officer who is in charge of the total management of the enterprise
CFO	The most senior official of the enterprise who is accountable for all aspects of financial management, including financial risk and controls and reliable and accurate accounts
Chief Operating Officer (COO)	The most senior official of the enterprise who is accountable for the operation of the enterprise
CRO	The most senior official of the enterprise who is accountable for all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk.
CIO	The most senior official of the enterprise who is responsible for aligning IT and business strategies and accountable for planning, resourcing and managing the delivery of IT services and solutions to support enterprise objectives
Chief Information Security Officer (CISO)	The most senior official of the enterprise who is accountable for the security of enterprise information in all its forms
Business Executive	A senior management individual accountable for the operation of a specific business unit or subsidiary
Business Process Owner	An individual accountable for the performance of a process in realising its objectives, driving process improvement and approving process changes
Strategy (IT Executive) Committee	A group of senior executives appointed by the board to ensure that the board is involved in, and kept informed of, major IT-related matters and decisions. The committee is accountable for managing the portfolios of IT-enabled investments, IT services and IT assets, ensuring that value is delivered and risk is managed. The committee is normally chaired by a board member, not by the CIO.
(Project and Programme) Steering Committees	A group of stakeholders and experts who are accountable for guidance of programmes and projects, including management and monitoring of plans, allocation of resources, delivery of benefits and value, and management of programme and project risk
Architecture Board	A group of stakeholders and experts who are accountable for guidance on enterprise architecture-related matters and decisions, and for setting architectural policies and standards
Enterprise Risk Committee	The group of executives of the enterprise who are accountable for the enterprise-level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the enterprise risk committee.
Head of HR	The most senior official of an enterprise who is accountable for planning and policies with respect to all human resources in that enterprise
Compliance	The function in the enterprise responsible for guidance on legal, regulatory and contractual compliance
Audit	The function in the enterprise responsible for provision of internal audits
Head of Architecture	A senior individual accountable for the enterprise architecture process
Head of Development	A senior individual accountable for IT-related solution development processes
Head of IT Operations	A senior individual accountable for the IT operational environments and infrastructure
Head of IT Administration	A senior individual accountable for IT-related records and responsible for supporting IT-related administrative matters
Programme and Project Management Office (PMO)	The function responsible for supporting programme and project managers, and gathering, assessing and reporting information about the conduct of their programmes and constituent projects
Value Management Office (VMO)	The function that acts as the secretariat for managing investment and service portfolios, including assessing and advising on investment opportunities and business cases, recommending value governance/management methods and controls, and reporting on progress on sustaining and creating value from investments and services
Service Manager	An individual who manages the development, implementation, evaluation and ongoing management of new and existing products and services for a specific customer (user) or group of customers (users)
Information Security Manager	An individual who manages, designs, oversees and/or assesses an enterprise's information security
Business Continuity Manager	An individual who manages, designs, oversees and/or assesses an enterprise's business continuity capability, to ensure that the enterprise's critical functions continue to operate following disruptive events
Privacy Officer	An individual who is responsible for monitoring the risk and business impacts of privacy laws and for guiding and co-ordinating the implementation of policies and activities that will ensure that the privacy directives are met. Also called data protection officer.

Fig. 5.15 Roles in COBIT 5. Source: ISACA, COBIT 5, www.isaca.org/COBIT

5.3.4 Management Practices and Inputs/Outputs

The management practices as defined in the RACI chart (see previous section) each are assigned inputs and outputs (Fig. 5.16). Inputs are pieces of information (documentation) required for the management practice to operate effectively and efficiently. Outputs are deliverables of a successful operating management practices

Process Practices, Inputs/Outputs and Activities				
Management Practice	Inputs From	Description	Outputs Description	To
DSS02.01 Define incident and service request classification schemes.	APO09.03	SLAs	Incident and service request classification schemes and models	Internal
Define incident and service request classification schemes and models.	BAI10.02	Configuration repository	Rules for incident escalation	Internal
	BAI10.03	Updated repository with configuration items	Criteria for problem registration	DSS03.01
	BAI10.04	Configuration status reports		
	DSS01.03	Asset monitoring rules and event conditions		
	DSS03.01	Problem classification scheme		
	DSS04.03	Incident response actions and communications		

Fig. 5.16 Inputs and outputs of processes. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

Activities
<ol style="list-style-type: none"> 1 Define incident and service request classification and prioritisation schemes and criteria for problem registration, to ensure consistent approaches for handling, informing users and conducting trend analysis. 2 Define incident models for known errors to enable efficient and effective resolution. 3 Define service request models per service request type to enable self-help and efficient service for standard requests. 4 Define incident escalation rules and procedures, especially for major incidents and security incidents. 5 Define incident and request knowledge sources and their use.

Fig. 5.17 Activities in a process. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

expressed in information elements or documentation. The COBIT manual also provided information as where the inputs originated from and where the outputs should go to.

As an example, the management practice DSS02.01 “Define incidents and service request classification scheme” requires as input “Service Level Agreements.” If the management practice operates well, it will deliver as output “rules for incident escalation.” This deliverable is required for all other management practices within this process (as indicated by the label “internal”).

5.3.5 Management Practices and Activities

Finally, each management practice is decomposed into a set of required activities. These activities should be seen as a potential set of required activities that are needed to “implement” the management practice in the organization. The level of detail of these activities often corresponds to that of other related detailed frameworks, such as in the case of this example process under review clearly refer to ITIL (Fig. 5.17).

5.4 Translating COBIT to Your Practice

COBIT did develop a generic framework, suitable for “any” organization. It does contain a lot of valuable information but by first reading the documentation it may be difficult to grasp the essence and/or the practical elements. For a practical approach it is important for an organization to rework and extract the necessary information and transform it to an organization-specific template or approach, suitable for its size, culture, industry, etc.

5.4.1 Scoping COBIT

Some processes may be more important for one organization than another. The process DS 4—*ensure continuous service* for example will be of high importance in a financial organization. Indeed, if the IT systems of a commercial bank are not available for a certain time, this may have a negative impact on the financial results of the bank. On the contrary the same process will most probably have a lower priority for a bricks & stones factory, resulting in lower maturity level requirement. It is as such important that before starting with a COBIT implementation, there needs to exist a clear set of enterprise goals and IT goals to scope COBIT down to the specific needs of the organization (see infra). Once a prioritized list of COBIT processes is identified (based on the enterprise goals and IT-related goals), the organization can consider to perform a quick assessment on the current maturity of these processes and then decide to work on those processes first that were identified as highly important (based on the enterprise goals and IT-related goals) but also low in maturity (based on the quick assessment).

5.4.2 Turning COBIT Process into Practice: Example EDM2—Benefits Delivery

Once specific processes are selected, the information provided in COBIT 5 needs to be translated into organization-specific approaches. For example, in the process EDM2: Ensure Value Delivery, COBIT 5 references the need to define and communicate portfolio and investment types, categories, and criteria (see activity 1 in Fig. 5.18). This is about understanding which types of IT-related investment can be done and which criteria will be used to prioritize them.

In the case of a major Belgian Bank, these investment types were identified as shown below. Next to the production budget, there are three types of investment: maintenance projects (small break/fix projects), continuity project (enhancements), and more complex investments (typically across business units) (Fig. 5.19).

This typology is closely aligned to terminology often used in the consultancy words, specifically “run,” “grow,” and “transform” projects. For the “investment

EDM02 Process Practices, Inputs/Outputs and Activities (cont.)						
Governance Practice	Inputs		Outputs			
	From	Description	Description	To		
EDM02.02 Direct value optimisation. Direct value management principles and practices to enable optimal value realisation from IT-enabled investments throughout their full economic life cycle.			Investment types and criteria	AP005.01 AP005.03		
			Requirements for stage-gate reviews	BAI01.01		
Activities						
1. Define and communicate portfolio and investment types, categories, criteria and relative weightings to the criteria to allow for overall relative value scores.						
2. Define requirements for stage-gates and other reviews for significance of the investment to the enterprise and associated risk, programme schedules, funding plans, and the delivery of key capabilities and benefits and ongoing contribution to value.						
3. Direct management to consider potential innovative uses of IT that enable the enterprise to respond to new opportunities or challenges, undertake new business, increase competitiveness, or improve processes.						
4. Direct any required changes in assignment of accountabilities and responsibilities for executing the investment portfolio and delivering value from business processes and services.						
5. Define and communicate enterprise-level value delivery goals and outcome measures to enable effective monitoring.						
6. Direct any required changes to the portfolio of investments and services to realign with current and expected enterprise objectives and/or constraints.						
7. Recommend consideration of potential innovations, organisational changes or operational improvements that could drive increased value for the enterprise from IT-enabled initiatives.						

Fig. 5.18 Example process EDM 2: ensure benefits delivery. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

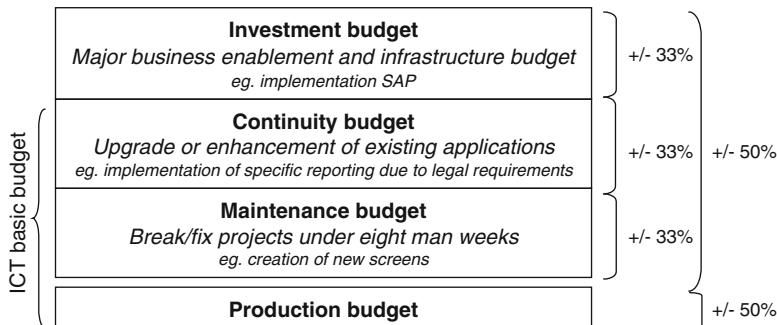


Fig. 5.19 Types of investment at major bank

Return on investment	Alignment with strategy	Competitive advantage/need	Necessity (legal, organ.)	Reduces operat. risks
Support management	Project and organis. risks	Support future informat. architecture	Functional uncertainty	Technical uncertainty

Fig. 5.20 Investment criteria in major bank. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

projects,” the bank agreed upon a set of tangible and intangible investment criteria, which were derived from the “information economics” concepts (see Chap. 4) (Fig. 5.20).

5.4.3 Turning COBIT Process into Practice: Example APO5—Portfolio Management

Once the investment criteria are set, COBIT 5 proposes in the subsequent process APO5—Portfolio Management to “perform detailed assessment of all programme business case” (see activity 2 at the bottom of Fig. 5.21).

Management Practice	Inputs		Outputs			
	From	Description	Description	To		
AP005.03 Evaluate and select programmes to fund. Based on the overall investment portfolio mix requirements, evaluate and prioritise programme business cases, and decide on investment proposals. Allocate funds and initiate programmes.	EDM02.01	<ul style="list-style-type: none"> Evaluation of investment and services portfolios Evaluation of strategic alignment 	Programme business case	AP006.02 BAI01.02		
	EDM02.02	Investment types and criteria	Business case assessments	AP006.02 BAI01.06		
	AP003.01	Architecture concept business case and value proposition	Selected programmes with ROI milestones	EDM02.01 BAI01.04		
	AP004.04	Proof-of-concept scope and outline business case				
	AP006.02	Budget allocations				
	AP006.03	<ul style="list-style-type: none"> Budget communications IT budget and plan 				
	AP009.01	Identified gaps in IT services to the business				
	AP009.03	Service level agreements (SLAs)				
	BAI01.02	<ul style="list-style-type: none"> Programme benefit realisation plan Programme mandate and brief Programme concept business case 				
Activities						
<ol style="list-style-type: none"> 1. Recognise investment opportunities and classify them in line with the investment portfolio categories. Specify expected enterprise outcome(s), all initiatives required to achieve the expected outcomes, costs, dependencies and risk, and how all would be measured. 2. Perform detailed assessments of all programme business cases, evaluating strategic alignment, enterprise benefits, risk and availability of resources. 3. Assess the impact on the overall investment portfolio of adding candidate programmes, including any changes that might be required to other programmes. 4. Decide which candidate programmes should be moved to the active investment portfolio. Decide whether rejected programmes should be held for future consideration or provided with some seed funding to determine whether the business case can be improved or discarded. 5. Determine the required milestones for each selected programme's full economic life cycle. Allocate and reserve total programme funding per milestone. Move the programme into the active investment portfolio. 6. Establish procedures to communicate the cost, benefit and risk-related aspects of these portfolios to the budget prioritisation, cost management and benefit management processes. 						

Fig. 5.21 Example process: portfolio management. *Source:* ISACA, COBIT 5, www.isaca.org/COBIT

Scoring investment files										
	Return	Alignment to strategy	Competitive advantage	Necessity	Legal necessity	Information architecture	Reduction operational risk	Project & organisational risk	Functional uncertainties	Technical uncertainties
Interest and liquidity risk project	red	green	green	green	green	green	green	green	red	red
Quantitative credit risk management project	green	green	green	green	green	red	red	red	red	red
Multichannel application project	green	green	green	yellow	yellow	green	green	green	green	green
ERP phase 2 project	red	green	green	green	green	yellow	green	red	red	yellow
...										

Fig. 5.22 Traffic light report for all investment projects

In the case of the bank in previous example, for each investment criterion (see top row in Fig. 5.22), a number of questions are developed (Fig. 5.22). The questions for “competitive advantage and need” for example are: “Does the programme deliver competitive advantage?” and “Is the programme a necessity to remain competitive?” The criterion gets a red, yellow, or green color if the average of the underlying questions for a specific investment (see first column in Fig. 5.22) score low, medium, or high. There is no overall average calculated over all criteria, so in this way, a kind of traffic light report is generated for each investment project, as visualized in Fig. 5.22.

This scoring is performed by the initiator of the investment project, in the case of the bank, the business architect. To obtain an objective measurement and a consistent scoring, all scores of all investments are always challenged and overviewed before they are consolidated prior to going to the Executive Committee.

To be able to execute the previous process, detailed business cases need to be developed for each of the proposed investment initiatives. A possible approach or template to build up detailed business cases is provided below, and is part of the business case process as discussed in Chap. 4 (Fig. 5.23).

5.5 COBIT Process Maturity and Process Capability

Process maturity has been a core component of COBIT for more than a decade. Determining the level of process maturity for given processes allows organizations to determine which processes are essentially under control and which represent potential “pain points” (Debreceny & Gray, 2011).

The concept of process maturity in earlier versions of COBIT was based on the Software Engineering Institute’s Capability Maturity Model (Debreceny & Gray, 2011). In COBIT 5, process maturity has been replaced by the concept of process capability (ISACA, 2012; ISO/IEC, 2004). This is based on the ISO/IEC 15504 standard “Information technology—Process assessment” (SPICE). ISO/IEC 15504 and the process capability model in COBIT 5 *define six capability levels* (*0—Incomplete, 1—Performed, 2—Managed, 3—Established, 4—Predictable, 5—Optimizing*).

Within the Process Assessment Model (PAM) level 0, indicates that the IT process is not implemented or “fails to achieve its process purpose. At this level, there is little or no evidence of any systematic achievement of the process purpose.” At level 1 the “implemented process achieves its process purpose.” At level 1, however, the process cannot be said to be under control. At level 2, the process is “implemented in a managed fashion (planned, monitored, and adjusted) and its work products are appropriately established, controlled, and maintained.” At level 3, the process is implemented “using a defined process that is capable of achieving its process outcomes.” At level 4, the process “operates within defined limits to achieve its process outcomes,” and finally at level 5, the process is “continuously improved to meet relevant current and projected business goals” (ISACA, 2012, Chap. 8).

Cover Sheet	Implementation Approach (How?)
Programme name	Programme plan, milestones, and time frame
Business sponsor	Programme dependencies
Programme manager	Enterprise architecture compliance
Revision notes	Security policy compliance
Validation signatures	Critical success factors
Approval signature	Stage gate funding requests
Executive Summary	Resourcing requirements
Programme context	Governance arrangements
Name	Appendices
Business sponsor	The detailed programme plan (including individual project plans)
Track record of management team	The resourcing plan
Category of investment	The financial plan
Programme description/profile	The benefits realisation plan (including the benefits register)
Synopsis of business case assessment	The (organisational) change management plan
Programme contribution (value)	The risk management plan (including the risk register)
Programme plan and timing	
Change implications	
Key risks	
Comparative value summary	
Introduction / Background (Why?)	
Opportunity and problem definition (Why?)	
Problem to be addressed	
Purpose	
Strategic contribution	
Recommended Solution (What?)	
Scope	
Business impact	
Approach	
Alternatives	
Value Impact (Attractiveness)	
Financial and non-financial benefits	
Description	
Measures	
Accountabilities	
Costs (full economic life cycle, full IT and business costs, best/ worst/ most likely case)	
Organisational Change Implications (Feasibility)	
Breadth and depth of change	
Organisational capability and	
readiness	
Risks and Assumptions and their mitigation (Feasibility)	
Delivery risks	
Benefit risks	

Fig. 5.23 Business case template

The new PAM uses a measurement framework that is similar in terminology to the existing maturity models in COBIT 4.1. However, while the words are similar the scales are not the same. In this new assessment scheme, realizing a capability level 1 is already an important achievement for an enterprise. A process at PAM level 1 means that the goals of this process are achieved which is clearly different from the CMM Initial/Ad Hoc level 1. In the COBIT 4.1 maturity model, a process

could achieve a level 1 or 2, or even 3, without fully achieving the process's objectives. Conversely, in the COBIT 5 process capability level, this will result in a lower score of 0 or 1. This implies that assessments done under the PAM are likely to result in lower scores. A signal benefit of the new assessment model is the improved focus on confirming that a given process is actually achieving its purpose and delivering the required outcomes as expected. Although defining target capability levels is up to each enterprise to decide, many enterprises will have the ambition to have all their processes achieve at least capability level 1. Otherwise, what would be the point of having these processes?

5.6 COBIT 5 Product Family

ISACA has developed a set of books around the COBIT 5 knowledge base, as shown in Fig. 5.24. The core book is called “COBIT 5: A Business Framework for Governance and Management of Enterprise IT.” This book, which is freely available, describes the main five principles around the framework, also discussed in section “COBIT 5 Principles” in this book.

Next, for each of the enablers (process, structure, etc.), a specific guide is developed or will be developed. At the moment of writing of this book, the COBIT 5: Enabling Processes was available, as well as COBIT 5: Enabling Information. The Enabling Processes Guide is discussed in section “Translating COBIT to Your Practice” of this book. The Enabling Information Guide talks about how to manage information in the organization and how to understand and ensure quality of information (consistency, reliability, accuracy, etc.).

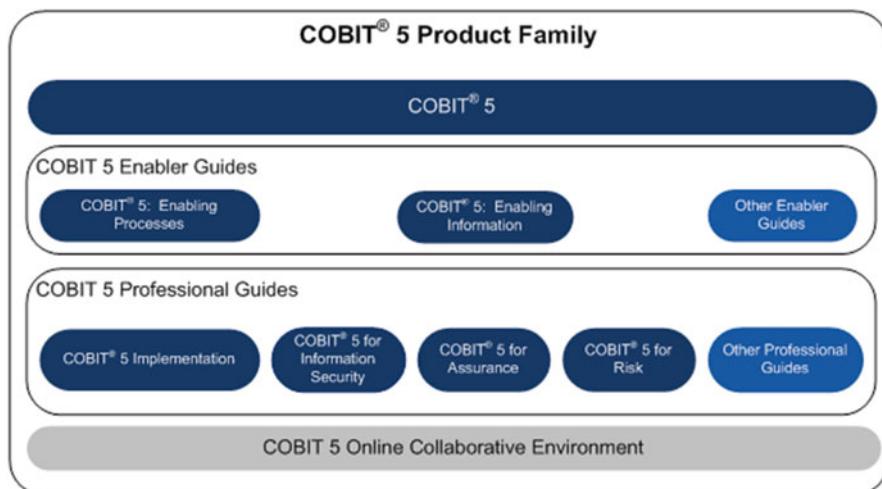


Fig. 5.24 COBIT 5 product family. Source: ISACA, COBIT 5, www.isaca.org/COBIT

Next, professional guides for specific audiences are developed including a generic guide on how to implement COBIT 5. More specific are COBIT 5 for Information Security and COBIT 5 for Risk, both looking at the information risk and security challenge in organization and they provide guidance, based on COBIT, on how to tackle these challenges. There is also a specific guide towards the use of COBIT 5 for audit and assurance purposes, which is discussed in the following chapter of this book. All the existing and upcoming publications can be viewed at www.isaca.org.

5.7 COBIT 5 Benchmarking

During the writing of this book, a research project was running at the University of Antwerp—Antwerp Management School (commissioned by ISACA) which included international benchmarking on the implementation status (0=not implemented; 5=fully implemented) of the COBIT 5 Enablers and more specifically, the COBIT 5 processes. An international data set of 894 responses was collected across different industries, sectors, and sizes.

Figure 5.25 shows that overall, organizations have implemented the enablers related to structures and services/infrastructure/applications the best. As expected, more complex enablers such as processes and certainly culture and ethics received lower implementation scores.

Looking at the process enabler in more detail (see Fig. 5.26) it appears that organizations have best implemented the more “IT factory” related processes situated in the delivery and support (DSS) area. More strategic- and governance-related processes, situated in the EDM domain, clearly achieved lower implementation scores. The latter is certainly consistent with the discussion on “IT Governance and The Board” as discussed in Chap. 2, which also pointed out the “surprising state of practice” of board engaging in enterprise governance of IT.

More benchmarking results can be obtained by contacting the authors of the book. These benchmarking results will also be made available through other publications in academic- and business-oriented journals.

Summary

In 2012 a new version of COBIT, the international best practice framework for governance of enterprise IT, was released. COBIT 5 primarily is a framework made by and for practitioners, but in the past decade, it has also incorporated many insights coming from IT and general management literature, including concepts and models such as “strategic alignment,” “balanced scorecard,” “IT savviness,” and “organizational systems.” By clearly indicating how the core elements of COBIT 5 are built on these IT and general management insights, this chapter sought to contribute to a better understanding of the COBIT 5 framework, and provide guidance

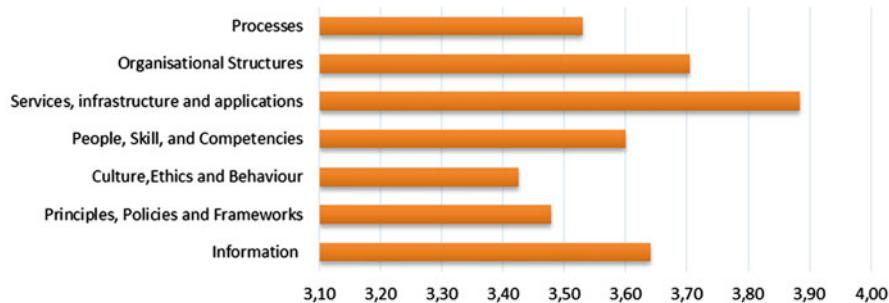


Fig. 5.25 Benchmarking implementation status of COBIT 5 enablers

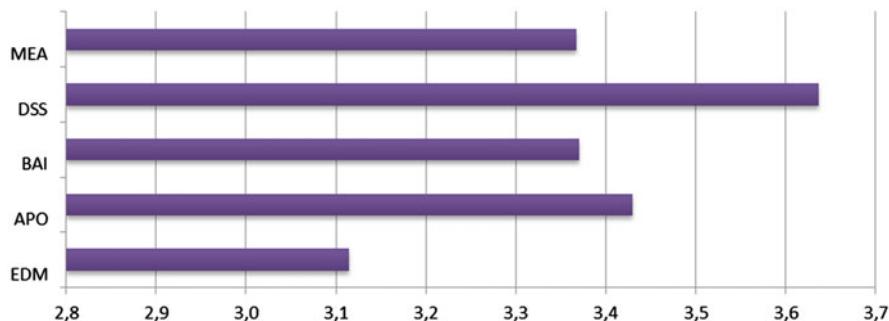


Fig. 5.26 Benchmarking implementation status of COBIT 5 processes

to practitioners in their endeavors to apply COBIT 5 as an instrument to improve governance and management of enterprise IT in their organizations.

Study Questions

1. Explain why COBIT should be regarded as a framework that enables the implementation of Enterprise Governance and Management of IT.
2. Explain the concept of “enablers” suggested by COBIT 5.
3. Explain how the IT-balanced scorecard concepts are integrated in COBIT.
4. Explain how the concept of “IT savviness” is introduced in COBIT 5.
5. Explain why COBIT 5 can be seen as a “holistic” framework for enterprise governance of IT?
6. Explain the difference between governance and management of enterprise IT and illustrate with examples.

References

- De Haes, S., & Van Grembergen, W. (2008). An exploratory study into the design of an IT governance minimum baseline through Delphi Research. *Communications of AIS*, 22, 443–458.
- 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.
- De Haes, S., & Van Grembergen, W. (2010). Prioritising and linking business goals and IT goals in the financial sector. *International Journal of IT/Business Alignment and Governance*, 1(2), 47–67.
- De Wit, B., & Meyer, R. (2005). *Revolving strategy paradoxes to create competitive advantage*. London: Cengage Learning EMEA.
- Debreceny, R. S., & Gray, G. L. (2011). IT governance drivers of process maturity. In *7th University of Waterloo Symposium on Information Integrity and Information Systems Assurance*. Toronto, ON, Canada: Center for Information Integrity and Information Systems Assurance, University of Waterloo.
- ISACA. (2007). *COBIT 4.1*. Retrieved from www.isaca.org
- ISACA. (2008). *Val IT 2.0*. Retrieved from www.isaca.org
- ISACA. (2009). *RISKIT*. Retrieved from www.isaca.org
- ISACA. (2012). *COBIT 5*. Retrieved from www.isaca.org
- ISO/IEC. (2004). *15504:2004: Information technology—Process assessment*. Retrieved from www.iso.org
- ISO/IEC. (2008). *38500:2008: Corporate governance of information technology*. Retrieved from www.iso.org
- Kaplan, R. S., & Norton, D. P. (1996). *The balanced scorecard: Translating strategy into action*. Boston: Harvard Business School Press.
- Peterson, R. (2004). Crafting information technology governance. *Information Systems Management*, 21(4), 1–16.
- Van Grembergen, W., & De Haes, S. (2009). *Enterprise governance of IT: Achieving strategic alignment and value*. New York: Springer.
- Van Grembergen, W., De Haes, S., & Van Brempt, H. (2007). How does the business drive IT? Identifying, prioritising and linking business and IT goals. *Information Systems Control Journal*, 6, 1–5.
- Van Grembergen, W., De Haes, S., & van Brempt, H. (2008). *Understanding how business goals drive IT goals*. Retrieved from www.isaca.org
- Van Grembergen, W., Saull, R., & De Haes, S. J. (2003). Linking the IT balanced scorecard to the business objectives at a major Canadian Financial Group. *Journal for Information Technology Cases and Applications*, 5(1), 23–45.
- Weill, P., & Ross, J. (2009). *IT savvy: What top executives must know to go from pain to gain*. Boston: Harvard Business Press.

Chapter 6

COBIT as a Framework for IT Assurance

Abstract In the previous chapter, COBIT was introduced and discussed as a powerful framework to implement Enterprise Governance of IT. However, COBIT also provides in-depth support to execute IT assurance/audit assignments. This chapter explains how the COBIT concepts can be leveraged in the context of IT assurance. Readers, who are not familiar with COBIT, are recommended to first read Chap. 5 where the concepts of COBIT are explained. A lot of material in this section is based on the “COBIT 5 For Assurance” Guide (ISACA, 2013, www.isaca.org).

6.1 IT Assurance and COBIT 5

In COBIT 5, “assurance” is defined as follows (ISACA, 2012a, b; ISACA, 2013; Van Grembergen & De Haes, 2009): “Assurance means that, pursuant to an accountability relationship between two or more parties, an IT audit and assurance professional may be engaged to issue a written communication expressing a conclusion about the subject matters to the accountable party.”

This definition implies that an assurance assignment comprises five components:

- A three-party relationship, including
 - The accountable party (auditee), the person or group accountable for the subject matter under review.
 - The user of the assurance report, in some cases this can be the same party as the accountable party.
 - The assurance professional, who executes the assurance assignment.
- The subject matter: The subject matter refers to the areas within the audit universe that will be under review in the assurance assignment. These areas can include all aspects of the seven COBIT 5 enablers, i.e., structures, processes, policies, etc. (see previous chapter).

Characteristic	Self-assessment	Internal Audit/Compliance Review	External Audit
Independence requirements	<ul style="list-style-type: none"> • Not required or guaranteed • Objectivity of self-assessors should be encouraged by defining clear responsibilities and correct follow-up. 	Should be optimised by the correct composition of the internal audit/compliance department members	Independence of the external auditors should be established, verified and maintained.
Interested party (user)	Enabler owners	Executive management, audit committee, operational management and enabler owners involved	Primarily directed toward the board/shareholders, but of importance to the enterprise in general
Responsible party (accountable party)	Enabler owners	Management and business enabler owners involved	The board and executive management involved
Assurance provider (assurance professional)	Enabler owners	Internal audit/compliance department	External auditor
Reporting format and requirements	<ul style="list-style-type: none"> • Free format • Internal consistency required 	Internal consistency required, in line with professional standards	Highly regulated/standardised
Governing rules/standards	Standardised approaches based on good practices required	<ul style="list-style-type: none"> • Standardised approaches based on good practices required • Professional standards and code of ethics to be respected 	Adherence to applicable codes of ethics and standards should be established, verified and maintained.
Level of trust (reliability)	<ul style="list-style-type: none"> • Lowest • Depends on the skill and objectivity of the assessor 	<ul style="list-style-type: none"> • Medium • Depends on the skill and expertise of the internal audit/compliance department and on co-operation of the accountable party 	Maximal

Fig. 6.1 Types of assurance engagements. *Source:* COBIT 5 for Assurance, www.isaca.org

- Suitable criteria: These criteria are the reference against which the subject will be evaluated. In principle, management determines what the evaluation criteria are, but the assurance professional can of course also assess the appropriateness of the proposed evaluation criteria.
- The assurance process: Assurance professionals follow a specific structured process when executing an assurance assignment. This process is discussed in detail further in this chapter.
- Conclusions and recommendations: Based on the observations, facts, and documentation, the assurance professionals will analyze the data, identify control weaknesses and root causes, and substantiate the risks. These findings will be brought together in the assurance report, potentially also including specific recommendations.

COBIT 5 distinguishes between different types of assurance engagements, ranging from self-assessment to external audits (see Fig. 6.1). Self-assessments are typically executed by management and are more open in structure and format. External audits on the other hand are often more regulated and deliver more objective data and assessments.

In its “COBIT 5 for Assurance” book, COBIT developed two perspectives on assurance:

- The first perspective discusses how to build an assurance function in the organization, leveraging the seven enablers proposed by COBIT. For example, what types of structures are required, such as the audit committee, what policies are to be considered such as an audit charter, etc.

- The second perspective focuses on the execution of the assurance process itself and how the auditors can provide assurance over each of the seven enablers (process, structures, etc.). For example, how to provide assurance over the “information security” process in an organization.

Both perspectives are further discussed in this chapter.

6.2 Building an IT Assurance Function

As discussed in previous chapter, COBIT 5 presents seven enablers that are required to address organizational challenges in a holistic manner. In the “COBIT 5 For Assurance” guide, this insight is applied to the question of how to build and organize the IT assurance function in an organization. This implies that questions are answered such as:

- Which structures do we require, e.g., audit committee?
- Which processes do we require, e.g., the assurance process?
- Which policies do we require, e.g., audit charter?
- ...

In the next sections, we provide some examples for each of the seven enablers, as discussed in the “COBIT 5 for Assurance” guide.

6.2.1 Structures for IT Assurance

“COBIT 5 for IT Assurance” does present some structures that are essential in building up an IT assurance function, including the audit committee at the level of the board of directors, the audit department, a compliance department, etc. Figure 6.2 gives an overview of such structures for IT assurance.

For each of those structures, the COBIT document provides more detailed guidelines. As in the example of Fig. 6.3, the structure and composition of the audit

Structure	Definition/Description
Board/audit committee	The governance body that is charged with evaluating, directing and monitoring the organisation's audit, risk management and control functions. The board (or the equivalent function that is charged with the governance of the enterprise) often delegates responsibility for providing assurance to the audit committee, whose members are usually drawn from the board (non-executives). Final accountability, however, stays with the board.
Audit department	The function in the enterprise responsible for provision of internal audits ³
Compliance department: • Regulatory • Internal	• Regulatory —The function in the enterprise responsible for guidance on legal, regulation and statutory requirements, and contractual compliance • Internal —The group responsible for verifying compliance with organisational policies and standards
External audit	The function responsible for provision of external audit and associated services

Fig. 6.2 Structures for IT assurance. Source: COBIT 5 for Assurance, www.isaca.org

Composition	
Role	Description
Members of the board	A limited number of members of the board will be members of the audit committee (usually non-executives).
Financial/auditing specialist	An independent expert in accounting/audit
Mandate, Operating Principles, Span of Control and Authority Level	
Area	Characteristic
Mandate	Focuses on aspects of financial reporting and on the entity's processes to manage business and financial risk and for compliance with significant applicable legal, ethical and regulatory requirements. The mandate will be detailed in the audit charter.
Operating principles	<ul style="list-style-type: none"> • The audit committee will meet at least quarterly. More frequent meetings may be scheduled during specific initiatives or when issues need to be dealt with on a very urgent basis. • Audit committee members can have informal contact with key management members (e.g., CEO, CFO, chief audit executive, lead external audit partner) to more quickly react to situations. • The audit committee reports quarterly to the board of directors on significant issues and actions for remediation/improvement. • Minutes of all meetings should be kept and approved in a timely manner.
Span of control	The audit committee is servicing the entire legal entity for which the board is responsible.
Authority level/decision rights	The audit committee is responsible for oversight of: <ul style="list-style-type: none"> • Financial reporting and accounting • Regulatory compliance • Risk management • The internal audit function • The effectiveness of the internal control processes
Delegation rights	The audit committee delegates authority to the audit department to carry out the internal audit plan.
Escalation path	All key issues and findings impacting the board's decision making need to be escalated to the board.

Fig. 6.3 Composition and operation of the audit committee. *Source:* COBIT 5 for Assurance, www.isaca.org

committee is discussed, and its mandate defined as a function that: “focuses on the aspects of financial reporting and on the entity’s processes to manage business and financial risks and for compliance with significant applicable legal, ethical, and regulatory requirements.”

6.2.2 Processes for IT Assurance

The IT assurance function also requires some IT assurance processes. To identify those processes, the “COBIT 5 for Assurance” guide refers to the “COBIT 5: Enabling Processes” book (see also previous chapter). The core assurance processes are to be found in the MEA (Monitor, Evaluate, Assess) area, more specifically MEA 2—Monitor, Evaluate, and Assess the System of Internal Control.

For these core assurance processes, the “COBIT 5 for Assurance” book provides extra guidance. Figure 6.4 illustrates an example for MEA 2.08—Execute Assurance Initiatives, where a distinction is made in the assurance processes (see activity 3 and 4) between verifying control design versus verifying operating effectiveness (see also further in this chapter) Next, typical inputs (e.g., risk assessment) and outputs (e.g., audit reports) are proposed that are required in the assurance process.

Management Practice	Inputs		Outputs					
	From	Description	Description	To				
MEA02.08 Execute assurance initiatives. Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risk.	AP011.05	Root causes of quality delivery failures	Refined scope	EDM05.01 All APO All BAI All DSS All MEA				
	AP012.04	Risk analysis and risk profile reports for stakeholders						
	AP012.06	Risk-related root causes	Assurance review results	EDM05.03 All APO All BAI All DSS All MEA				
	DSS05.02	Results of penetration tests	Assurance review report	EDM05.03 All APO All BAI All DSS All MEA				
	DSS06.01	Root cause analyses and recommendations						
	MEA03.03	Identified compliance gaps						
Activities and Detailed Assurance Activities								
1. Refine the understanding of the IT assurance subject.								
2. Refine the scope of key control objectives for the IT assurance subject.								
3. Test the effectiveness of the control design of the key control objectives.								
3.1 Assess the enabler design, i.e., assess to what extent expected good practices are applied.								
3.2 Assessment will include the following steps:								
• Observe/inspect and review the enabler approach, and test the design for completeness, relevancy, timeliness and measurability.								
• Enquire whether and confirm that the responsibilities for the enabler and overall accountability have been assigned. Test whether accountability and responsibilities are understood and accepted. Verify that the right skills and the necessary resources are available.								
• Enquire through interviews with involved key staff members whether the enabler mechanism, its purpose, and the accountability and responsibilities are understood.								
3.3 Additionally and specifically in internal audit assignments, the cost-effectiveness of the enabler design should/could be verified with the following assurance steps:								
• If the design of the enabler is effective, investigate whether it can be made more efficient by optimising steps, looking for synergies with other enablers and reconsidering the balance of prevention vs. detection and correction. Consider the effort spent in maintaining the enablers.								
• If the enabler set is operating effectively, investigate whether it can be made more cost-effective.								
4. Alternatively/additionally test the outcome of the key control objectives.								
4.1 Assess whether the expected outcomes for each of the enablers in scope are achieved, i.e., assess the effectiveness of the enabler (control effectiveness).								
4.2 Assess to what extent the enabler life cycle is well-managed.								
4.3 To test the outcome or effectiveness of the enabler, the assurance professional needs to look for direct and indirect evidence of the impact on the enabler goals. This implies the direct and indirect substantiation of measurable contribution of the enabler to the IT-related goals, thereby recording direct and indirect evidence of actually achieving the expected outcomes.								
4.4 The assurance professional should obtain direct or indirect evidence for selected items/periods by applying a selection of testing techniques to ensure that the enabler under review is working effectively. The assurance professional should also perform a limited review of the adequacy of the enabler results and determine the level of substantive testing and additional work needed to provide assurance that the enabler performance is adequate.								
MEA02 Process Practices, Inputs/Outputs, Activities and Detailed Assurance Activities (cont.)								
Activities and Detailed Assurance Activities (cont.)								
5. Document the impact of control weaknesses.								
6. Communicate with management during execution of the initiative so that there is a clear understanding of the work performed and agreement on and acceptance of the preliminary findings and recommendations.								
7. Supervise the assurance activities and make sure the work done is complete, meets objectives and is of an acceptable quality.								
8. Provide management with a report (aligned with the terms of reference, scope and agreed reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.								

Fig. 6.4 Details of a core assurance process. Source: COBIT 5 for Assurance, www.isaca.org

Next to the presented core assurance processes, some supporting assurance processes can be considered, as presented in Fig. 6.5. For example, the process “manage budget and costs” is required to ensure that the assurance function defines and maintains its budget. The process “manage relationship” refers to the need to build and maintain good relationships between the auditors and the auditees in the organization.

Process Identification	Reasoning	Assurance-specific Outputs
EDM01 Ensure governance framework setting and maintenance.	The assurance function requires the establishment of a governance structure.	<ul style="list-style-type: none"> • Stakeholder requirements with regards to governance of assurance • Assurance guiding principles • Assurance function and audit committee mandate • Formal documentation on assurance decisions • Formal meeting minutes of assurance management meetings
EDM02 Ensure benefits delivery.	The enterprise must ensure that the assurance function generates value.	<ul style="list-style-type: none"> • Formal documentation of stakeholder requirements • Formal documentation of assurance function's contribution to business objectives • Feedback on delivery of assurance initiatives
EDM03 Ensure risk optimisation.	The enterprise must ensure that assurance-related risk is managed.	Remedial actions to address assurance deviations noted
EDM05 Ensure stakeholder transparency.	The assurance function is an important provider of overall stakeholder transparency.	<ul style="list-style-type: none"> • Evaluation of assurance reporting requirements • Assurance summary of activities to audit committee
AP002 Manage strategy.	The assurance function must develop a strategy for providing assurance. The strategy should be aligned with the business strategy.	<ul style="list-style-type: none"> • List of potential assurance function coverage gaps • Assurance function capabilities • Criteria for prioritizing gaps in assurance coverage • Assurance function requirements in target IT capabilities • Assurance function gaps to be closed • Assurance function capability benchmark • Assurance strategic plan • Updated IT strategic plan and road map taking into account the assurance function requirements • Annual assurance function plan
AP006 Manage budget and costs.	The assurance function must budget for its activities and supporting systems.	<ul style="list-style-type: none"> • Assurance activity prioritization • Assurance function budget
AP007 Manage human resources.	The assurance function requires the right number of people and skills.	<ul style="list-style-type: none"> • Assurance function requirements for the staffing process • Assurance function training plan • Assurance function personnel evaluations • Resource performance tracking plan and indicators, resource allocation plan
AP008 Manage relationships.	Relationships between the assurance function and business are critical.	<ul style="list-style-type: none"> • Understanding of business processes of the enterprise • Strategy to obtain stakeholder commitment • Assurance communication strategy • Assurance action plans for the business
AP011 Manage quality.	Quality improvement is an essential component of effective assurance provisioning.	<ul style="list-style-type: none"> • Relevant assurance good practices and standards • Assurance function quality standards • Assurance function quality metrics agreed upon • Results of external quality peer reviews of the assurance functions • Assurance function quality metrics implemented in line with industry good practices • Documented root causes for assurance issues with quality metrics
AP012 Manage risk.	Assurance risk (audit risk) must be managed.	<ul style="list-style-type: none"> • Data for assurance risk analysis • Assurance function risk analysis results • Enterprise risk profile that includes assurance-related aspects • Risk evaluation and assessment strategies • Updated enterprise risk profile
BAI08 Manage knowledge.	Assurance function must be provided with the knowledge required to support assurance staff in their work activities.	<ul style="list-style-type: none"> • Updated classification of assurance function information • Published knowledge repositories • Updated access control over assurance information • Updated rules for assurance information disposal

Fig. 6.5 Supporting IT assurance processes. Source: COBIT 5 for Assurance, www.isaca.org

6.2.3 Principles, Policies, and Frameworks for IT Assurance

The assurance function also requires supporting principles, policies, and frameworks. Many publications exist around this topic, with ISACA (www.isaca.org) and IIA (www.theiia.org) being important references. A specific reference goes to the “IT Assurance Framework (ITAF)” as developed by ISACA (www.isaca.org/itaf), which gives a relatively complete overview of required IT assurance policies,

Principles, Policies and Frameworks Area	Covered by
Code of professional ethics	ITAF, 2 nd Edition, Section 1
General standards	1001 Audit Charter 1002 Organisational Independence 1003 Professional Independence 1004 Reasonable Expectation 1005 Due Professional Care 1006 Proficiency 1007 Assertions 1008 Criteria
Performance standards	1201 Engagement Planning 1202 Risk Assessment in Audit Planning 1203 Performance and Supervision 1204 Audit Materiality 1205 Audit Evidence 1206 Using the Work of Other Experts 1207 Irregularities and Illegal Acts
Reporting standards	1401 Reporting 1402 Follow-up Activities

Fig. 6.6 Principles, policies, and frameworks for IT assurance. *Source:* COBIT 5 for Assurance, www.isaca.org

principles, and frameworks. As shown in Fig. 6.6, ITAF describes a code of ethics, general standards relating to the audit charter and independency, performance standards concerning materiality of the audit work, standards in terms of reporting, etc. The “COBIT 5 for Assurance” guide does not provide more guidance around these topics but does give all the necessary reference to find more information.

6.2.4 Culture, Ethics, and Behavior for IT Assurance

The required and expected behavior for the IT assurance function is represented at three levels: the organization, the assurance professional, and management. Figure 6.7 for example posits that it is important that the organization supports the idea of transparency and a culture of participation (behavior 3). For the assurance professional, it is in turn important that he/she regularly informs stakeholders about the progress of the assurance assignment (behavior 8). Management finally needs to clearly understand and consider the risks when they are making business decisions (behavior 10).

6.2.5 Information for IT Assurance

The IT assurance function requires appropriate information to be able to work well. Specific examples are the “audit charter” which defines the boundaries in which the audit group will work, and the “risk strategy” which defines how the organization looks at risk. More examples of information elements are illustrated in Fig. 6.8.

For each information element, quality attributes are defined. For example, the audit charter needs to be accurate, relevant, available, etc. (see Fig. 6.9).

Ref.	Behaviour	Key Objective/Suitable Criteria/Outcome
Enterprise-wide		
1	Has a risk and compliance-aware culture throughout, including the proactive identification and escalation of risk.	Must define a risk management approach and risk appetite. Zero tolerance of non-compliance with legal and regulatory requirements must be established.
2	Promotes and executes continuous improvement.	Must embed the concept of continuous improvement in its business-as-usual activities.
3	Has transparent and participative culture as an important focus point.	Actions must engender a core enterprise value of transparency and participation.
4	Develops and supports a clearly defined structure for ethical responsibility and a culture that promotes specific accountability.	Must establish a zero-tolerance approach for non-ethical behaviours.
5	Proactively engages the assurance partners to support the general recognition of the need for and importance of the value of assurance.	Business decision making and planning must consider assurance and compliance an integral element of the achievement of the business objectives.
Assurance professional		
1	Maintains a continuous professional education.	Identifies and allocates appropriate time for and takes advantage of continuous professional educational opportunities. Funding and support is provided by the organisation to maintain and expand assurance knowledge.
2	Focuses on key areas of risk.	Maintains an adequate knowledge of the business and relevant technologies to support assurance activities.
3	Has an awareness of cultural (geographical, ethnic, social, etc.) differences.	Must understand the context for business, technology and cultural differences relevant to assessment activities.
4	Maintains active communication with and a positive approach toward auditees.	Must maintain an effective relationship that drives candid discussions to promote remediation of assurance issues and avoidance of unnecessary risk.
5	Maintains continuous engagement to ensure appropriate alignment.	Should promote use of a common taxonomy and understanding of risk.
6	Maintains a mutually productive and influential relationship with key stakeholders.	Must influence the identification, discussion, debate and reduction of risk by maintaining a professional and influential relationship with the key stakeholders.
7	Reports on key risk in clear, concise and effective manner.	Must communicate risk in terms that are understandable to the listeners.
8	Keeps relevant stakeholders informed in a timely manner.	Must compile, analyse, format and distribute assurance material on a timely basis.
Management		
1	Values and funds assurance activities.	Must recognise the need for audits and risk assessments and the value they bring. Must ensure an appropriate level of resources.
2	Shares business plans and objectives, and involves assurance in key strategic decisions.	Must ensure that the assurance function is involved in strategic planning.
3	Maintains positive relationship with assurance partners.	Must maintain active, candid and constructive communications with the assurance functions on all aspects of business-as-usual activities.
4	Embraces assurance findings and performs root cause analysis.	Must promote openness; provide funding, knowledge and time; and demonstrate willingness to remediate the root cause of assurance findings.
5	Involves relevant stakeholders to resolve issues and implement solutions in a timely manner.	Must effectively balance short-term and firefighting activities with long-term sustainable solutions. Additionally, management must ensure a clear and concise accountability to drive sustainable solutions.
6	Promotes awareness of the importance of an effective control environment.	Must promote awareness of a proactive risk- and self-aware culture and commitment to create the same.
7	Openly debates to reach the right level of risk appetite.	Must promote and embrace an open, candid and inclusive communication culture, which includes all relevant stakeholders and risk partners. Additionally, management must clearly define the risk appetite and ensure an appropriate level of debate as part of business-as-usual activities.
8	Demonstrates ethical leadership and sets the tone at the top.	Must implement a code of ethics across the enterprise and promote a culture of ethical behaviour.
9	Identifies systemic issues in a timely manner and fully discloses them to assurance.	Must ensure that self-assessment and assurance routines identify issues in a timely manner. Management must also ensure that such issues are fully disclosed to relevant stakeholders.
10	Understands the risk impact of their decisions.	Must implement a comprehensive risk management framework that appropriately aligns to all relevant stakeholders and risk partners. This risk framework must clearly and concisely identify, define and quantify risk in terms relevant to the enterprise.

Fig. 6.7 Expected behavior and culture for the IT assurance function. *Source:* COBIT 5 for Assurance, www.isaca.org

Information Item	Definition/Description of Information Items Needed to Support the Assurance Function
Assurance templates	Guide completion of key assurance activities, such as scopes, audit/assurance programmes, findings registers and assurance reporting
Audit charter	Provides the functional and organisational framework within which the enterprise internal audit group operates. The charter sets out the nature, role, scope, status, authority and responsibility of the internal audit group.
Audit committee assurance report	Is used to summarise the outcomes of the assurance activities, e.g., completion status of the audit plan, proposed audit plan changes, summary finding statistics, resolution of findings information and other relevant matters of note
Audit plan	Offers a framework that includes all specific assurance activities for a defined period of time. Should clearly document the objectives of the assurance initiative and key inputs such as risk assessments, business strategies and priorities, and should be developed in conjunction with management and executives and be approved by the board/audit committee.
Audit strategy	Defines clear assurance objectives as well as scope and focus of the assurance approach. For example, independent objective assurance is provided to the board through the audit committee and to executive management.
Compliance plans	Should include all specific compliance activities. Each type of compliance plan should clearly document the objectives of the compliance initiatives and key inputs such as risk assessments, business strategies and priorities.
Compliance strategy	Defines clear compliance objectives as well as scope and focus of the compliance approach
Financial and budgetary requirements	Consists of assurance budget requirements, such as HR, travel and tools
HR competencies framework	Identifies the key assurance competency levels and certifications
IT assurance universe	Defines the area of responsibility of the IT assurance provider. It is usually based on a high-level structure that classifies and relates enterprise enablers, allowing for a risk-based selection of discrete IT assurance initiatives. The assurance universe must be defined at the enterprise level.
Legal and regulatory factors	Collection of all legal and regulatory factors influencing the assurance initiatives.
Risk strategy	Defines clear risk objectives as well as scope and focus of the risk approach
Risk register	Encompasses risk planning outcomes, defining entity-level risk profiles, including consequences, likelihoods and control effectiveness ratings

Fig. 6.8 Information elements for IT assurance. Source: COBIT 5 for Assurance, www.isaca.org

Goals	Quality Subdimension and Goals	Description (The extent to which information is ...)	Relevance	Expected Outcome
	Intrinsic			
	Accuracy	correct and reliable	High	Information is correct and reliable.
	Objectivity	unbiased, unprejudiced and impartial	High	Audit objectives are well-defined and measurable.
	Believability	regarded as true and credible	High	Information is highly regarded in terms of its source or content.
	Reputation	regarded as true and credible	High	Information is factually correct.
Contextual and Representational	Relevancy	applicable and helpful for the task at hand	High	Information meets board/audit committee needs.
	Completeness	not missing and is of sufficient depth and breadth for the task at hand	High	Information includes full consideration of board/audit committee requirements.
	Currency	sufficiently up to date for the task at hand	High	Information is refreshed periodically.
	Amount of Information	appropriate in volume for the task at hand	Low	
	Concise Representation	represented in a concise manner	Low	
	Consistent Representation	presented in the same format	Low	
	Interpretability	in appropriate languages, symbols, and units, and the definitions are clear	High	Information is clear and relevant.
	Understandability	easily comprehended	High	Information is adapted to be comprehensible by target audience.
Security	Manipulation	easy to manipulate and apply to different tasks	High	It is easy to leverage information.
	Availability	available when required, or easily and quickly retrievable	High	Information is easily available.
	Restricted Access	restricted appropriately to authorised parties	High	The access to this information item is determined by the chief audit executive and is restricted as follows: <ul style="list-style-type: none">• Write access: chief audit executive• Read access: all other stakeholders

Fig. 6.9 Quality requirements for the audit charter. Source: COBIT 5 for Assurance, www.isaca.org

6.2.6 Services, Infrastructure, and Applications for IT Assurance

“COBIT 5 for Assurance” proposes some typical assurance services and applications. Typical supporting assurance services are “time tracking and reporting,” enabling the assurance professional to manage and track its resources, and “reporting and communication” which also covers the typical workflow systems to capture data, write reports, etc. (Fig. 6.10)

In terms of applications (Fig. 6.11), certainly CAATS (Computer Assisted Audit Techniques) need to be mentioned, which are applications that can fully or partially automate specific audit assignments.

Ref.	Service	Description
1	Reporting and communication	Report writer and workflow system that facilitates the writing, review, editing, approvals, and attestation of assurance materials
2	Quality assurance services	Scoring assessment of assurance work to ensure level of quality is maintained in accordance with assurance objectives
3	Time tracking and reporting	Recording of resource utilisation by project and assurance activity to help effectively manage engagements and as historical information to be used for planning
4	Business resource engagement	Ability to assess the need, identify and make available business resources vital in completing assurance work
5	Access services for information	Ability to request and obtain access to information required to complete assurance work
6	Law and regulation tracking services	Ability to identify, assess and relate compliance requirements to the enterprise
7	Emerging risk advisory services	Ability to identify and track new types of risk to influence how assurance work is performed
8	Performance evaluation process	Ability to evaluate performance of assurance professionals against established skills requirements

Fig. 6.10 Supporting services for IT assurance. *Source:* COBIT 5 for Assurance, www.isaca.org

Ref.	Supporting Application	Description
1	Risk model repository	Highlights, tracks, and documents rationale associated with key inherent and residual risk
2	Computer-assisted audit techniques (CAATs)—tools	Applications used to automate the audit process
3	Audit practices library	A library that contain standards, sampling techniques, guidelines, procedures and templates for use by assurance professionals
4	Document management systems	A library that can store, archive and document assurance work performed, such as work papers and assurance evidence
5	Planning tool	Applications that allow assurance professionals to plan, schedule, resource and ensure maintenance of adequate cycle coverage of risk
6	Tracking issues system	A repository that captures issues (and supporting detail) and helps manage the life cycle from remediation to resolution
7	Data analytics/sampling techniques	Data mining and statistical methods that support sampling, tools and techniques
8	Workflow systems	Ability to route assurance material for review, comments, approval and attestations

Fig. 6.11 Supporting applications for IT assurance. *Source:* COBIT 5 for Assurance, www.isaca.org

6.2.7 People, Skills, and Competencies for IT Assurance

Finally, IT assurance professionals need to have the appropriate skills and competencies in specific areas, including:

- Strategy and planning
- Engagement and resource planning
- Assessing and testing
- Enterprise expertise
- Risk management and risk management framework
- Interpersonal and relationship management
- Understanding of standards, guidelines, and procedures
- Communication (oral, presentation, and written)
- Audit practices
- Data management and data quality
- Analytics
- Programme and project management
- Interview and investigation
- System development life cycle
- Basic IT concepts
- Resilience
- Specific technical expertise

For each of those areas, the “COBIT 5 for Assurance” guide develops the required skills and competencies, including the typically expected degrees and certifications; For example, for the skills set “assessing and testing,” reference is made to ISACA certificates such as CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), and CGEIT (Certified in the Governance of Enterprise IT) (Fig. 6.12).

6.3 Executing the IT Assurance Process

The second part of the “COBIT 5 for Assurance” guide addresses how the IT assurance process can be executed. As such, this section further develops the “MEA-2—Executive Assurance Initiatives” process, and it proposes three parts:

1. Determining the scope of the assurance assignment
2. Understanding the subject matter, selecting the evaluation criteria, and executing the assessment
3. Communicating and reporting the results

Description	
The ability to assess information and develop and perform appropriate tests to achieve assurance objectives is a core skill for the assurance professional	
Experience, Education and Qualifications Required	
Requirement	Description
Experience	Appropriate experience as an assurance professional
Qualifications	CISA, CISM, CGEIT (one or more)
Knowledge, Technical and Behaviour Skills	
Requirement	Description
Knowledge	<ul style="list-style-type: none"> • Analytics • Performance measurement • International standards • IT basic understanding—security and application control risk, architecture, networking, development life cycle, etc. • Emerging threats
Technical skills	<ul style="list-style-type: none"> • Time management skills • Data analytics • Data mining
Behavioural skills	<ul style="list-style-type: none"> • Effective communicator—written and oral • Process-oriented • Relationship builder • Culturally aware • Problem solver • Effective time manager • Detail-oriented

Fig. 6.12 Required skills for IT assessing & testing. *Source:* COBIT 5 for Assurance, www.isaca.org

6.3.1 Determining the Scope of the Assurance Assignment

In the first phase, the assurance professional needs to determine the scope of the assurance assignment. The assurance professional evaluates who the involved stakeholders are and what the stakes are of each of them. Next, specific objectives for the assurance assignment can be agreed upon. These objectives can be expressed in terms of the IT-related risks and opportunities toward achieving enterprise goals. Depending on the agreed-upon objectives, the specific scope of the assurance assignment can be set, articulating which processes, structures, policies, and other enablers will be assessed.

Consider the example of an assurance scope for assessing “internet banking,” more specifically regarding the question whether internet banking is safe for the bank. The involved stakeholders in this case range from the board of directors up to IT management roles. Relevant IT goals that are selected for this case are “Manage IT-related business risks” and “security of information.” The selected enablers in scope include structures such as the IT development department, processes such as APO10-Manage suppliers and policies such as the security policy.

It should be clear that the cascade developed in COBIT 5, linking enterprise goals to IT-related goals and processes, can be very instrumental in determining an appropriate scope in the context of specific IT goals and/or enterprise goals.

6.3.2 Executing the IT Assurance Initiative

In the execution phase, two steps are crucial: understanding the subject matter and performing the assessment steps.

It is indeed important that the assurance professional has a good understanding and knowledge over the subject matter he/she is going to assess. ISACA has developed more detailed guidance on each of the seven enablers (processes, structures, etc.) they propose, and of course this information will be helpful in understanding the subject matter.

Next, the appropriate assurance steps need to be executed. “Testing Control Design” (often also referred to as “testing the design effectiveness”) covers the assurance steps to be performed to assess the adequacy of the design of controls. This assurance activity includes the evaluating of the appropriateness of control measures for the process under review by considering identified criteria, industry standard practices, and applying professional judgment.

Figure 6.13 provides examples for the COBIT process BAI6—*Manage changes*, as derived from the management practices and activities presented in the “COBIT 5—Enabling Processes” guide (see Chap. 5). The first assurance steps provided is “Enquire whether and confirm that the change management process allows business process owners and IT to request changes to infrastructure, systems, or applications.” These assurance steps typically are based on interviews with key stakeholders in the organization, leading to narratives describing the control measures applied in the organization.

The “COBIT 5 for Assurance” guide refers to typical generic testing methods such as enquire, confirm, observe, and inspect. “Enquire and confirm” is about asking management questions to obtain an understanding of the processes and/or applications and includes the search and examination of exceptions and deviations. “Observe” is about the observation and description of the processes and procedures. “Inspect” includes the review of plans, policies, and procedures, the tracing of

- Enquire whether and confirm that the change management process allows business process owners and IT to request changes to infrastructure, systems or applications.
- Enquire whether and confirm that the overall change management process includes emergency change procedures (e.g., defining, raising, testing, documenting, assessing and authorising emergency changes).

Fig. 6.13 Testing the control design

Nature of Control	Frequency of Performance	Minimum Sample Size
Manual	Many times per day	25
Manual	Daily	25
Manual	Weekly	5
Manual	Monthly	2
Manual	Quarterly	2
Manual	Annually	1
Automated	Test one application of each programmed control activity (assures IT general controls are effective).	
IT general controls	Follow the guidance above for manual and programmed aspects of IT general controls.	

Fig. 6.14 Guidance for sample size selection

transactions through the processes/systems, physically inspection of the presence of documentation and assets,

To identify to key interviewees in this assurance process, the assurance professional can leverage COBIT's RACI charts, looking for those people who are in the first place accountable (A) and responsible (R) (see Chap. 5) for these activities. Further, when asking for documentation the assurance professional can consult the inputs/outputs tables of COBIT, giving information on typical documentation to be expected in the process under review.

After “testing the control design,” “Testing the outcome of control objectives” (often also referred to as “testing the operational effectiveness”) addresses the assurance steps to be performed to ensure that the control measures established are working as prescribed, consistently and continuously. These assurance steps typically are about inspecting samples, recalculations, etc. When looking for documentation to retrieve “evidence” in these activities, the assurance professional can consult the inputs/outputs tables of COBIT, giving information on typical documentation to be expected in this process.

The testing of the outcome in many cases is performed on the basis of samples. There are many factors that determine sample sizes. Figure 6.14 represents a common sample size used in practice by auditors to test the operating effectiveness of controls.

Figure 6.15 provides examples for the COBIT process BAI6—*Manage changes*, such as “inspect a selection of changes and determine if requests have been categorized.” Again, these questions are derived from the management practices and activities as defined in the “COBIT 5—Enabling Processes” guide.

6.3.3 Communicate and Report

If control weaknesses are identified based on previous steps, “Testing the impact of the control weaknesses” encompasses the assurance steps to document and report on potential business risks if specific control objectives are not met. Main issue here is that the assurance professional should not just report on control weaknesses (e.g., “we found evidence that there is no project management methodology”),

- Inspect a selection of changes and determine if requests have been categorised.
- Inspect a selection of changes and determine if changes have been prioritised based on predefined criteria.
- Inspect a selection of changes and determine if changes have been assessed in a structured method (e.g., security, legal, contractual and compliance implications are considered and business owners are involved).
- Inspect a sample of emergency changes and verify that they have been processed in accordance with the change management framework. Verify that procedures have been followed to authorise, document, revoke access after change has been applied.

Fig. 6.15 Testing the outcome of control objectives

- Assess the time and cost of lack of formal change management standards and procedures (e.g., improper resource allocation, unclear roles and responsibilities, security breaches, lack of rollback procedures, lack of documentation and audit trails, inadequate training).
- Assess the time and cost of lack of formal impact assessment to prioritise and authorise changes.
- Assess the time and cost of lack of formal emergency change standards and procedures (e.g., compromised security, failure to properly terminate additional access authorisations, unauthorised access to corporate information).

Fig. 6.16 Testing the impact of control weaknesses

but the assurance professional should demonstrate what the potential business impact of these weaknesses is (e.g., the likelihood of IT project failing increases, causing budgets overruns or a longer time-to-market). Typical examples are provided in Fig. 6.16 for the example of the COBIT process BAI6—*Manage changes*. In most cases, the assurance professional tries to estimate the potential cost, loss of time, business impact, etc. due to the control weaknesses. The IT assurance professional can leverage COBIT’s goals and metrics tables to clarify the business issues at risk.

6.4 IT Assurance in Practice

To execute IT assurance activities in practice, templates can be very helpful in supporting the assurance execution. These templates can be simple in nature, and as an illustration, some (nonprescriptive) examples are provided in this section, specifically in support of the scoping and testing execution activities. Next section will also illustrate how some specific COBIT content components (without being exhaustive) can be helpful in the IT assurance work.

6.4.1 Templates for Scoping

When starting a specific assurance assignment, the detailed scope needs to be set first. As explained earlier, this scope analysis can be based on the identification and linking of relevant enterprise goals and IT-related goals (see left section of Fig. 6.17, where enterprise and IT-related goals can be defined and mapped), and derived from that, a set of IT-related (COBIT) processes in scope (see right section of Fig. 6.17, e.g., the five most important IT processes supporting the defined IT goals) (see also Sect. 5.4 on COBIT scoping).

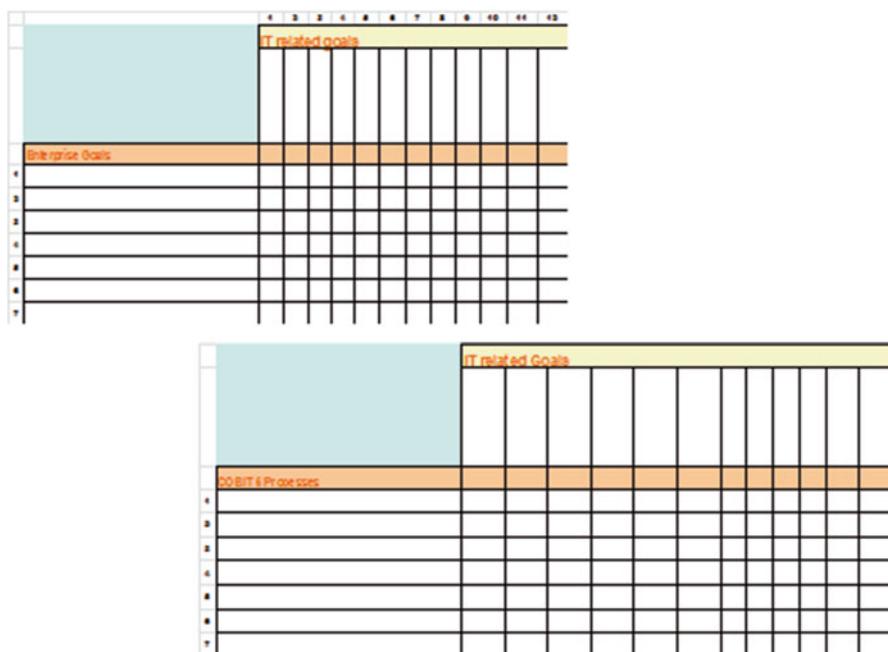


Fig. 6.17 Templates for value-based scoping

Risk																		
							Who does it?											
Importance	Performance							IT	Other	Outside	Do Not Know	Audited	Formality	Who is accountable?				
COBIT 5 Domains and Processes																		
Governance Evaluate, Direct and Monitor																		
EDM01 Ensure Governance Framework Setting and Maintenance																		
EDM02 Ensure Benefits Delivery																		
EDM03 Ensure Risk Optimisation																		
EDM04 Ensure Resource Optimisation																		
EDM05 Ensure Stakeholder Transparency																		
Management Align, Plan and Organise																		
APO01 Manage the IT Management Framework																		
APO02 Manage Strategy																		
APO03 Manage Enterprise Architecture																		
APO04 Manage Innovation																		
APO05 Manage Portfolio																		
APO06 Manage Budget and Costs																		
APO07 Manage Human Resources																		
APO08 Manage Relationships																		
APO09 Manage Service Agreements																		
APO10 Manage Suppliers																		
APO11 Manage Quality																		
APO12 Manage Risk																		
APO13 Manage Security																		

Fig. 6.18 Templates for risk-based scoping

Based on previous scoping exercise, a set of COBIT processes is deducted from a value perspective (value-based scoping, i.e., processes in support of the achievement of enterprise and IT goals). Depending on the context, it can be that this scope needs to be refined based on some risk insights and analysis. As an example, easy-to-use templates can be leveraged that indicate a high-level risk profile for processes, based on a quick evaluation of the importance and performance, and an indication of how responsibilities and accountabilities are assigned and organized (e.g., formality, etc.), as illustrated for two COBIT domains in Fig. 6.18.

Once the set of processes is defined, a set of management practices within each process needs to be selected, as a basis for the control framework. In support of this, attributes can be considered that help in evaluating and comparing the importance of management practices within a COBIT process. These attributes are:

- Expedience, i.e., the speed and ease it takes, on average, to implement the control objective; e.g., a high (H) score means the control objective can be implemented quickly.
- Sustainability, i.e., the degree to which the control can continue to operate without maintenance and management attention due to changes in the environment, reduced discipline, changed priorities, etc. Automated procedures (e.g., automatic backup) and mechanisms where the stakeholder has a high expectation (e.g., a weekly performance report), are generally more sustainable over time than procedures and mechanisms that require a certain people's behavior and discipline.

- Effectiveness, i.e., the degree to which the control objective—compared to other control objectives for this process—contributes to achieving the process goals and mitigates the risks, irrespective of efficiency, cost, etc.
- Cost (effort), i.e., the investment in people and money to implement a control objective. There is usually a strong relationship between cost and expedience because high cost implies many activities and investments are required to implement the control objective which generally means that implementation will not be expedient.

6.4.2 *Templates for Testing*

Figure 6.19 provides a template for testing the control design, at the level of a specific management practice (example DSS2.1: service desk). Assurance steps are developed based on professional judgment and based on the activities as described for each COBIT management practice. Required contact persons for interviewing are defined based on COBIT's RACI chart, and documentation to be retrieved can be found in the input/outputs tables. The assurance steps are then translated into a detailed and organization-specific assurance approach (column “control design question”), describing exactly what needs to be done. After execution, findings that are conclusions are recorded. An elaborated example of this approach is provided in Fig. 6.19.

Figure 6.20 provides a template, with examples, for testing control objective outcomes for the same process. Again (column 1), assurance steps are developed and cross-checked against the COBIT management practices and activities, supplemented with RACI chart information and required documentation, and then translated into a specific operating effectiveness approach, findings, and conclusions.

Figure 6.21 finally provides an example template on how control weaknesses can be reported, providing a short description of the control weakness and how it was detected (findings), clarifying the business risk and its classification, ultimately leading to prioritized recommendation.

Management practice	Activity	Contact person	Control design question	Documentation required	Control design finding	Control design conclusion	
DSS2.02: record, classify and prioritise service request and incidents	Log all service requests and incidents.	Service desk manager Incident manager	2. Review the incident management procedure and verify whether all call are recorded.	Incident management procedure	The incident management procedure requires all incidents to be logged.	PASS	

Fig. 6.19 Templates for testing control design

	<i>Management practice</i>	<i>Activity</i>	<i>Contact person</i>	<i>operating effectiveness question</i>	<i>Documentation required</i>	<i>operating effectiveness finding</i>	<i>operating effectiveness conclusion</i>
DSS2.02: record, classify and prioritise service request and incidents	Log all service requests and incidents.	Service desk manager Incident manager	Inspect a sample of incidents and verify if they are all logged.	Incident management procedure	20 incidents were retrieved, only 5 of them were logged in an appropriate way.	FAIL	

Fig. 6.20 Templates for testing control objective outcomes

Findings	
Description	Detection
Not all incidents are logged in an appropriate way.	
	Inspection
Risk	
Description	Classification
There is not clear overview of how many incidents are open in the service desk and what classifications they have. This might lead to loss of incidents and wrong prioritization, with unsatisfied business users as result.	
	High
Recommendation	
Description	Priority
Acquire tool to log and manage incidents in an easy way.	1

Fig. 6.21 Templates for testing impact of control weaknesses

Assignment Box 6.1: Case Study

Case background

Delta Lighting Design (DLD), founded in 1989, creates and assembles high-quality lighting products. The major goal of the company is to develop lighting products that are unique in concept and that appeal to a broad audience. Major processes within DLD are product design and development, procurement and ordering of components, assembling, and sales. DLD recently developed a strategic road map to align its IT with its overall business strategy with the help of a local consulting firm. DLD needed to align its IT infrastructure, processes, and applications with its strategic goals. The company knew that to compete more effectively, it would have to improve its customer focus and supply chain efficiency and support these areas with transparent IT solutions, compliant with the company's strategic IT vision. The company's main goals in undertaking a transformation of its IT infrastructure and processes were to support the creation of a comprehensive business, achieve profitable growth, reduce costs, and improve customer focus and supply chain efficiency.

(continued)

Assignment Box 6.1: (continued)

With this clear vision of where it needed to go, DLD sought a consulting partner with expertise in the assembling industry to develop the business case for implementing new IT infrastructure and processes, including recommendations for new major IT application installations and integration across its functional areas.

The consultancy firm teamed with DLD to deliver the company's IT strategy plan, including the business case for required investments.

The team used the consultant's proprietary methodology to evaluate DLD's strategic IT processes. The resulting road map aligns the company's IT strategy with its larger business goals and addresses the business requirements and issues. The actual implementations of recommended IT solutions will be completed during the next 2 years, delivering a solid return on investment (ROI) once the implementation is completed. The most important part of the solution was the implementation of an enterprise resource planning (ERP) system. The common ERP system is the key to DLD's cost reductions and profitable growth through the integration of production, supply, and customer service. It is expected that through this ERP implementation, a better fusion between IT and business will be achieved, enabling a more efficient supply chain and improved logistics for purchasing and distribution. Further, DLD expects increased assembling efficiency by a more optimal labor utilization, purchase price reduction, significant cost reduction through consolidation into one IT platform, reduced application development time, and more efficient finance and administration through integrated business processes.

Case questions

You are the auditor for DLD:

1. You are confronted in this case with the IT strategy process. Identify which COBIT management practices are most appropriate to consider in designing an audit plan, and justify your selection of the relevant management practices.
2. The solution was to bring in an ERP package. Identify which COBIT management practices are most appropriate to consider in designing an audit plan, and justify your selection of the relevant control objectives.

Summary

COBIT 5 is a powerful framework to implement enterprise governance of IT. However, the same reference can be used to execute IT audit and assurance assignments.

The "COBIT 5 for Assurance" guide provides two interesting sections. In the first place, it discussed how an organization can build up an IT assurance function,

by addressing the appropriate assurance structures, processes, policies, etc. In the second place, the “COBIT 5 for Assurance” guide explains how COBIT 5 provides information that helps in scoping down and understanding a specific assurance assignment towards a specific subject matter. Based on that insight, assurance steps can be developed that verify control design and operating effectiveness of the controls environment in the organization.

Study Questions

1. Discuss the difference between IT audit and IT assurance.
2. Explain how COBIT can be used in IT assurance assignments.
3. Explain and discuss the two core testing activities—testing control design and testing outcome of the control objective. Illustrate with examples.
4. Explain how inputs/outputs, RACI charts, and goals & metrics can be helpful in executing IT assurance activities.
5. In reporting on control weaknesses, the assurance professional should focus on business risk issues. Explain and illustrate.

References

- ISACA. (2012a). *COBIT 5*. Retrieved from www.isaca.org
- ISACA. (2012b). *COBIT 5: Enabling processes*. Retrieved from www.isaca.org
- ISACA. (2013). *COBIT 5 for assurance*. Retrieved from www.isaca.org
- Van Grembergen, W., & De Haes, S. (2009). *Enterprise governance of IT: Achieving strategic alignment and value*. New York: Springer.

Chapter 7

Guidelines for the Implementation of Enterprise Governance of IT

Abstract There is no real “silver bullet” (the ideal way) for implementing and maintaining effective Enterprise Governance of IT within an organization. Having developed a high-level Enterprise Governance of IT model does not imply that governance is actually working in the organization. Conceiving the governance model is the first step, implementing it into the organization is the next challenging step. An important challenge is: how do you get started? This chapter provides some key success factors, guidelines to get started and outlines a balanced scorecard (BSC) for enterprise governance of IT, to manage and measure the outcome of the governance project. Readers, who are not familiar with the BSC perspective, should first read Chap. 4 on the IT BSC.

7.1 Key Success Factors in the Case of KLM

Earlier in this book, the case of KLM was discussed. Although all organizations, including KLM, face some unique challenges, concerns around effective governance of IT, and the realization of real business value from today’s significant and increasingly complex investments in IT are a universal concern. Other organizations can certainly benefit from the experiences and lessons learned by KLM in this area (De Haes et al. 2011).

The factors that have been key to KLM’s success to-date have been discussed throughout this document, and are summarized below. We recommend that all organizations with an interest in improving their governance of IT consider these factors, both in terms of assessing where they are today, and in planning the steps they need to take to improve their performance. The factors include:

- **Senior management commitment:** KLM’s success started with their senior management. They had a strong executive leadership team, who moved beyond awareness of a problem, through understanding the causes of the problem and what needed to be done, to commitment to a sustained programme of action which included both clearly communicating direction and priorities, and embedding a

“value driven” culture. They set the tone from the top, promoting teamwork and collaboration, and breaking down “silo thinking.”

- **Business engagement:** Effective enterprise governance of IT will not happen without adequate and appropriate business engagement. In KLM’s case, it was very instrumental to have a “business-oriented” CIO (coming out of the business). This further demonstrated senior management commitment, as well as establishing credibility and starting to break down the “we–they” thinking between the IT and the other parts of the business which, in turn, lead to greater engagement, collaboration, and partnership.
- **Distinguishing between the “what” and the “how”:** Making a clear distinction between, and defining respective roles and responsibilities, regarding the “what,” i.e., the demand side, versus the “how,” i.e., the supply side, and the “investment” versus the “continuity” budget was a difficult, but essential step on the journey.
- **Defining key principles and practices:** Developing a small, clearly defined, simple and well-communicated set of principles and practices for enterprise governance of IT, focused on putting the business in full control of all IT demand and IT spend. In developing these principles and practices, KLM did not get “bogged down” in academic discussions about the difference between principles and practices, but presented them in a pragmatic and practical way that “worked for KLM.” They also supported them with more detailed background information and internal documentation to explain the impact and consequences of each of the principles and practices.
- **Positioning demand functions in the business:** Embedding the demand functions (BDOs) in the business organization was key to having them really act as business representatives, and reinforced the business responsibility for, and ownership of the “what” decisions, and the results of those decisions.
- **Clear and transparent business drivers:** A clear and shared understanding of business drivers is critical in order to be able to prioritize investments, and enable the selection of “the right things.” KLM used an innovative methodology to help clarify their business drivers and make them transparent.
- **Standard business cases:** While, in some ways, the process of developing a business case is as important as the result, a standard template ensures that the content of the business case is consistent, comprehensive, and comparable. In KLM’s case, they developed a standard business case template as a mandatory instrument for all investments above 150,000 euro.
- **A strong front-end demand process:** KLM established a rigorous process (through the BDOs) with intense scrutiny applied to the front-end review of each idea, initiative and business case. This allowed them to allocate funds appropriately by prioritizing their investments in terms of their potential contribution to business drivers, and their ability to deliver them.
- **A clear and transparent portfolio management process:** In KLM’s case, the transparency of this process, with clarity of business drivers and investments’ contribution to those drivers, levelled the “playing field,” established trust between

all stakeholders, and avoided the traditional decibel, or relationship-based decision-making approach.

- **An evolutionary approach:** KLM-balanced theory and organizational and cultural reality by taking a pragmatic and practical approach, making well-defined but sometimes-small steps, each with their own benefits. They are continuing to evolve and move forward on their journey.
- **A strong support group:** There is a need for a function to support the implementation, adoption, and ongoing application and sustainment of value management principles and practices. In KLM's case, this was the CIO-Office, who helped coach and embed enterprise governance of IT thinking and practices into the organization.

7.2 Getting Started: Pain Points and Trigger Events

One of the challenges is to get started and to obtain management attention and commitment to improve enterprise governance of IT. In support of that, it can be helpful to identify and clarify typical pain points or trigger events in your organization (ISACA 2012).

New or revised enterprise governance of IT practices can typically solve or be part of a solution to the following symptoms or pain points. As such, they can act as a “burning platform” to get management attention:

- Business frustration with failed initiatives, rising IT costs, and a perception of low business value
- Significant incidents related to IT-related business risk, such as data loss or project failure
- Outsourcing service delivery problems such as agreed-on service levels not being consistently met
- Failure to meet regulatory or contractual requirements
- IT's limitations of the enterprise's innovation capabilities and business agility
- Regular audit findings about poor IT performance or reported IT quality of service problems
- Hidden and rogue IT spending
- Duplication or overlap between initiatives or wasting resources
- Insufficient IT resources, staff with inadequate skills, or staff burnout/dissatisfaction
- IT-enabled changes frequently failing to meet business needs and delivered late or over budget
- Multiple and complex IT assurance efforts
- Board members, executives, or senior managers who are reluctant to engage with IT or a lack of committed and satisfied business sponsors for IT
- Complex IT operating models

In addition to the symptoms described previously, other events in the enterprise's internal and external environments, such as the following, can signal or trigger a focus on enterprise governance of IT and drive it high on the enterprise agenda:

- Merger, acquisition, or divestiture
- A shift in the market, economy, or competitive position
- Change in business operating model or sourcing arrangements
- New regulatory or compliance requirements
- An enterprise-wide governance focus or project
- A new CIO, chief financial officer (CFO), chief executive officer (CEO), or board member
- External audit or consultant assessments
- A new business strategy or priority
- Desire to significantly improve the value to be gained from IT

7.3 Measuring and Managing the Process of Enterprise Governance of IT

Today many organizations are in the process of implementing a combination of Enterprise Governance of IT structures, processes, and relational mechanisms. An important aspect of the Enterprise Governance of IT implementation process is the measuring and evaluation part. It makes sense for CIOs, executive managers, and board members to oversee the Enterprise Governance of IT status: how well it is doing and how it can be improved. For this purpose, a balanced scorecard (BSC) can be developed as a performance measurement system for the Enterprise Governance of IT project as a whole, enabling strategies for further improvement. With an Enterprise Governance of IT BSC, organizations can empower their board, CEO, CIO, executive management, and the business and IT participants by providing them the necessary information to evaluate the Enterprise Governance of IT success and act upon to achieve a better alignment between business and IT and consequently reach better results. In this sense, the Enterprise Governance of IT scorecard can play an important role in an overall programme that should be in place to enhance IT and corporate governance.

7.3.1 Building an Enterprise Governance of IT BSC

Figure 7.1 displays the mission statements, objectives, and corresponding measures for the four dimensions of the proposed Enterprise Governance of IT BSC: corporate contribution perspective, stakeholder's perspective, operational excellence perspective, and future perspective. The BSC is not only a performance management system but also provides a management system when causal relationships between

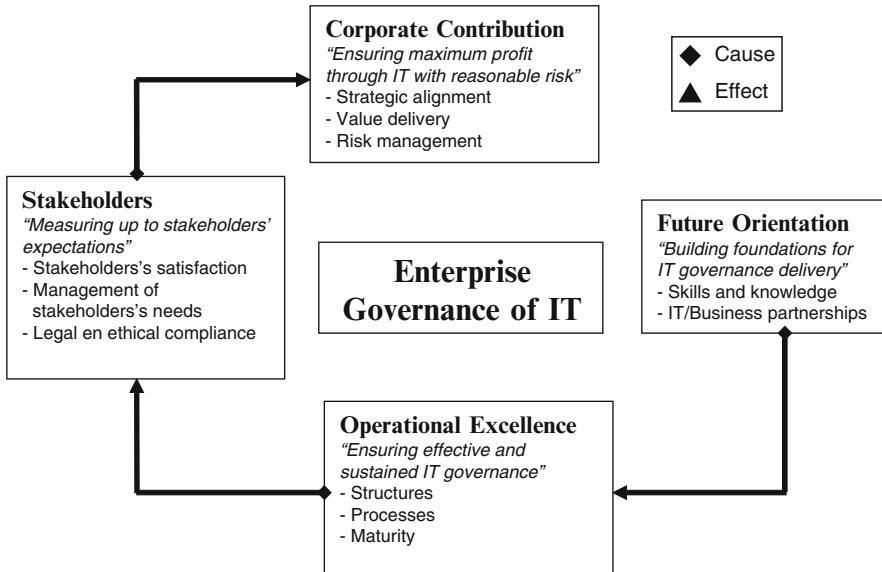


Fig. 7.1 Enterprise governance of IT scorecard perspectives and its cause-and-effect relationships

metrics are properly implemented. The ultimate goal of the development and implementation of an Enterprise Governance of IT project is the attainment of a better alignment between business and IT and consequently achieving better financial results (business value). It is therefore logical that the Enterprise Governance of IT BSC starts with a corporate contribution perspective. As shown in Fig. 7.1, the other three perspectives have a cause relationship with corporate contribution and among each other cause-and-effect relationships. An illustration of these coupled metrics in a cause-and-effect relationship is: overall completed Enterprise Governance of IT education (future orientation) may enhance the level of IT/business planning (operational excellence), which in turn may improve stakeholders' satisfaction (stakeholders orientation), and have a positive effect on the strategic match of major IT-enabled programmes (corporate contribution). The metrics of the main elements of Enterprise Governance of IT—structures, processes, and relational mechanisms—can be found in the operational excellence and future perspective dimensions.

7.3.2 Metrics for an Enterprise Governance of IT BSC

The **corporate contribution** dimension evaluates the performance of the Enterprise Governance of IT process: a well-balanced Enterprise Governance of IT process must enhance business profit through IT while mitigating the risk related to IT (mission). The three key objectives, as depicted in Fig. 7.2, are strategic alignment,

Perspective	Corporate Contribution	
Mission	Ensuring maximum profit while mitigating IT related risks	
Objectives	<i>Strategic Alignment</i>	
	Measures	Business/IT alignment maturity
		Strategic match of major IT projects
		Percentage of development capacity engaged in strategic projects
		Percentage of business goals supported by IT goals
	<i>Value Delivery</i>	
	Measures	Business unit performance management
		Business value of major IT projects based on ROI, NPV, IRR, PB
		Ratio IT costs/total turnover
		IT costs charged back to the business
	<i>Risk Management</i>	
	Measures	Number of new implemented IT security initiatives and security breaches
		Attainment of disaster recovery plans
		Number of IT audits performed and reported shortcomings

Fig. 7.2 Corporate contribution metrics

value delivery, and risk management, and are seen by the ITGI (2003) as main concerns of Enterprise Governance of IT.

The main measurement challenge is within the area of *strategic alignment*. As an overall metric, the *business/IT alignment maturity* model of Luftman is proposed (see Chap. 3). The measurement instrument is based on a survey to be completed by business and IT managers in the organization, addressing 22 attributes in six different domains: communication, competency and value measurement, governance, partnership, scope, and architecture and skills. The outcome is a business/IT alignment maturity score for the organization (see also Chap. 3). *Strategic match of major IT projects, percentage of development capacity engaged in strategic projects, and percentage of business goals supported by IT goals* are specific strategic alignment concerns. Measuring the strategic match of IT projects can be done through a scoring technique as introduced by Information Economics (see also Chap. 3): typical scores are attributed from 0 to 5 whereby 0 means no match at all and 5 a perfect match of the IT project with the business strategy.

In the *value delivery* area, *business unit performance measurement* refers to the business results of the individual lines of business. Indeed, the ultimate responsibility for achieving and measuring the business value rests with the business units. Alternative metrics for value delivery assessment are the traditional financial evaluations such as the return on investment, net present value, internal rate of return, and pay-back period (*business value of major IT projects based on ROI, NPV, IRR, and PB*). A major concern of senior management is the level of the IT costs and their recovery respectively measured through *ratio IT costs/total turnover* and *percentage of IT costs charged back to the business*.

Perspective	Stakeholders' Orientation																								
Mission	Measuring up to stakeholders' expectations																								
Objectives	Stakeholders' satisfaction																								
	<table border="1"> <tr> <td>Measures</td> <td>Stakeholders' satisfaction surveys on fixed times</td> </tr> <tr> <td></td> <td>Number of complaints of stakeholders</td> </tr> <tr> <td></td> <td>Index of availability of systems and applications</td> </tr> <tr> <td></td> <td><i>Management of stakeholders' needs</i></td> </tr> <tr> <td>Measures</td> <td>Number of meetings with stakeholders</td> </tr> <tr> <td></td> <td>Clear communication in place with CEO and board members</td> </tr> <tr> <td></td> <td>Index of CEO/board involvement in new and major IT initiatives</td> </tr> <tr> <td></td> <td>Number of major IT projects within SLA</td> </tr> <tr> <td></td> <td><i>Legal and ethical compliance</i></td> </tr> <tr> <td>Measures</td> <td>IT adherence to Sarbanes-Oxley Act</td> </tr> <tr> <td></td> <td>IT adherence to privacy regulations</td> </tr> <tr> <td></td> <td>Adherence to IT code of ethics/ IT code of conduct</td> </tr> </table>	Measures	Stakeholders' satisfaction surveys on fixed times		Number of complaints of stakeholders		Index of availability of systems and applications		<i>Management of stakeholders' needs</i>	Measures	Number of meetings with stakeholders		Clear communication in place with CEO and board members		Index of CEO/board involvement in new and major IT initiatives		Number of major IT projects within SLA		<i>Legal and ethical compliance</i>	Measures	IT adherence to Sarbanes-Oxley Act		IT adherence to privacy regulations		Adherence to IT code of ethics/ IT code of conduct
Measures	Stakeholders' satisfaction surveys on fixed times																								
	Number of complaints of stakeholders																								
	Index of availability of systems and applications																								
	<i>Management of stakeholders' needs</i>																								
Measures	Number of meetings with stakeholders																								
	Clear communication in place with CEO and board members																								
	Index of CEO/board involvement in new and major IT initiatives																								
	Number of major IT projects within SLA																								
	<i>Legal and ethical compliance</i>																								
Measures	IT adherence to Sarbanes-Oxley Act																								
	IT adherence to privacy regulations																								
	Adherence to IT code of ethics/ IT code of conduct																								

Fig. 7.3 Stakeholders metrics

Regarding the **risk management** objective, a high level of security and disaster recovery should be attained and measured by the *number of implemented IT security initiatives and security breaches* and *attainment of disaster recovery plans*. The audit performance is measured through *number of IT audits performed and reported shortcomings*.

Figure 7.3 portrays the objectives of the **stakeholder's perspective**: stakeholders' satisfaction, management of stakeholders' needs, and the legal/ethical compliance. This perspective evaluates the Enterprise Governance of IT process from the stakeholders' viewpoint including the board of directors, CEO and executive management, CIO and IT management, business and IT users, customers, shareholders, and the community. It is important to point out that the scope of this stakeholder's perspective is much broader than the customer perspective of an IT BSC (see Chap. 4).

In relation to **stakeholders' satisfaction** the scores from satisfaction surveys (*stakeholders' satisfaction survey on fixed times*) for the aforementioned categories of stakeholders can be used. This can also be applied to the *number of complaints of stakeholders*. An overall specific metric for business users is *index of availability of systems and applications*.

The **management of stakeholders' needs** are assessed through a set of performance metrics including measurements for the various stakeholder groups (*number of meetings with stakeholders*), more specific measurements for the board and CEO (*clear communication in place with CEO/board members* and *index of CEO/board involvement in new and major IT initiatives*), and specific measurements for the business users (*number of major IT projects within Service level agreement (SLA)*). SLAs, as already pointed out in the previous section, are an important governance instrument for enforcing levels of IT service that are acceptable by users and are attainable by their IT department and/or external providers.

Third objective within the stakeholder's perspective is the ***legal and ethical compliance***. In their publication on the board BSC, Epstein and Roy (2004) state that *the company's reporting strategy is a powerful driver of stakeholder satisfaction, so accountable companies should provide transparent reporting to their internal and external stakeholders, . . .* Accountability and transparency can be enhanced through the adherence to government and IT community regulations. The Sarbanes-Oxley (SOX) Act for example, focuses on the control and security of company's financial systems and consequently on its supporting IT processes. A crucial IT process in this context is "manage changes" as defined by COBIT, as this process should ensure that all changes to applications (incl. financial application) are done in a controlled manner (preventing for example changes that can lead to, or allow, fraudulent transactions). A specific metric for IT adherence to SOX could as such be the maturity level of the manage changes process evaluated on the basis of a maturity or capability model (see also Chap. 5).

The **operational excellence** perspective identifies the key Enterprise Governance of IT practices (structures and processes) to be implemented and their corresponding metrics. As defined before, structures refer to the existence of responsible functions and committees, and processes to decision-making and monitoring. The operational excellence card of Fig. 7.4 gives a variety of metrics for governance structures and processes including an overall IT governance maturity measurement.

For the **structures** area, three specific metrics regarding IT committees are retained: *number of meetings of IT strategy committee and IT steering committees, composition of IT committees, and overall attendance of IT committees*. Taking the criticality of IT into account, boards should manage IT with high commitment and accuracy as it does with other critical areas such as audit, compensation, and acquisitions.

Perspective	Operational Excellence	
Mission	Ensuring effective and sustained IT governance	
Objectives	Structures	
	Measures	Number of meetings of IT strategy committee and IT steering committees
		Composition of IT committees
		Overall attendance of IT committees
		CIO member of executive management
	Processes	
	Measures	Level of IT strategy planning and business planning
		Number of hours spent on IT/business strategic issues
		Existence of an IT balanced scorecard and a business balanced scorecard
		Number of IT processes measured through a scorecard
		Maturity of COBIT related processes
		Percentage of IT goals supported by COBIT processes
	Maturity	
	Measure	Overall level of the IT governance process maturity

Fig. 7.4 Operational excellence metrics

An instrument for achieving this is an IT strategy committee that supports the board in carrying out its IT governance duties. On the other hand, the detailed implementation of the IT/business strategies will be the responsibility of executive management assisted by a variety of steering committees overseeing major projects and managing priorities. Considering the importance of the IT strategy committee and the IT steering committees (see Sect. 2.1) these committees need careful and close monitoring through the aforementioned measures. Besides the meeting frequency and the attendance, it should be monitored whether the right people are members, taking into account factors such as their profile and IT literacy. An ideal composition of an IT strategy committee would be: a board member as chairman, other board members, nonboard independent members and ex-officio representation of key executives. *CIO member of executive management* is an indication of how important IT is considered within the organization.

The metric examples of the **processes** objective are focused on the level of and involvement in IT/business planning, the use of scorecards, and the maturity of COBIT processes. *Level of IT strategy planning and business planning* can be monitored by the effective use of strategic models such as the competitive forces model and the value chain of Porter and the Strategic Alignment Model of Henderson and Venkatraman. As already illustrated in previous section, the BSC can be an effective management instrument. The *existence of an IT BSC and a business BSC* is very supportive for achieving a linkage between IT and business objectives. Establishing such a cascade of scorecards with rolling-up and aggregating metrics of the IT scorecard in the business BSC may help to realize the ultimate link between IT and business. This cascade mechanism can also be used between the IT scorecard and scorecards on a lower level for the different IT processes (metric: *number of IT processes through a scorecard*). Regarding COBIT, *Percentage of IT goals supported by IT (COBIT) processes and their related maturity* is proposed.

The operational excellence card concludes with an **Enterprise Governance of IT maturity evaluation**. *Overall level of the Enterprise Governance of IT process maturity* can be assessed through the IT governance maturity model of ITGI. Such a maturity model provides a method for scoring that enables an organization to grade itself from nonexistent (level 0) to optimized (level 5). According to this model (see Fig. 7.5), organizations that are situated in level 0 are characterized by a complete lack of any recognizable IT governance process. To move up to level 1, the organization needs to at least recognize the importance of addressing IT governance issues. Maturity level 5 at least implies an advanced and forward-looking understanding of IT governance issues and solutions, supported by an established framework and best practices of structures, processes, and relational mechanisms. Maturity models such as the ITGI model have to comply with the basic principles of maturity measurement: one can only go to a higher maturity when all conditions described in a certain level are fulfilled. The level that an organization should target is of course dependent on the nature of the business: a business within the banking sector should probably strive to a higher IT governance level than a concrete factory.

0 Non Existent. Complete lack of any recognisable processes. Organization has not even recognised that there is an issue to be addressed.

1 Initial. There is evidence that the organization has recognised that the issues exist and need to be addressed. There are however no standardised processes but 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 chaotic.

2 Repeatable. Processes have developed to the stage where similar procedures are followed 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. Procedures have been standardised and documented, and communicated through training. It is however left to the individual to follow these processes, and any deviations would be unlikely to be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

4 Managed. It is possible to monitor and measure compliance with procedures and to take 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 Optimised. Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organizations. IT is used in an integrated way to automate the workflow and provide tools to improve quality and effectiveness.

Fig. 7.5 Generic IT governance maturity model. *Source:* ITGI, 2003, Board Briefing on IT Governance, second edition, from www.itgi.org

Perspective	Future Orientation										
Mission	Building foundations for IT governance delivery										
Objectives	Skills and knowledge										
	<table border="1"> <thead> <tr> <th>Measures</th><td>Number and level of cross-functional business/IT training sessions</td></tr> </thead> <tbody> <tr> <td></td><td>Number of overall Enterprise Governance of IT training sessions</td></tr> <tr> <td></td><td>Percentage completed Enterprise Governance of IT education per skill type</td></tr> <tr> <td></td><td>Number of Enterprise Governance of IT presentations for CEO and board members</td></tr> <tr> <td></td><td>Level and use of Enterprise Governance of IT knowledge management system</td></tr> </tbody> </table>	Measures	Number and level of cross-functional business/IT training sessions		Number of overall Enterprise Governance of IT training sessions		Percentage completed Enterprise Governance of IT education per skill type		Number of Enterprise Governance of IT presentations for CEO and board members		Level and use of Enterprise Governance of IT knowledge management system
Measures	Number and level of cross-functional business/IT training sessions										
	Number of overall Enterprise Governance of IT training sessions										
	Percentage completed Enterprise Governance of IT education per skill type										
	Number of Enterprise Governance of IT presentations for CEO and board members										
	Level and use of Enterprise Governance of IT knowledge management system										
IT/business partnership											
	<table border="1"> <thead> <tr> <th>Measures</th><td>Percentage of senior managers IT literate</td></tr> </thead> <tbody> <tr> <td></td><td>Percentage of IT managers business literate</td></tr> <tr> <td></td><td>Level of business perception of IT value</td></tr> </tbody> </table>	Measures	Percentage of senior managers IT literate		Percentage of IT managers business literate		Level of business perception of IT value				
Measures	Percentage of senior managers IT literate										
	Percentage of IT managers business literate										
	Level of business perception of IT value										

Fig. 7.6 Future orientation metrics

The **future orientation** scorecard reports on the building foundations for governance delivery focusing on relational mechanisms. Relational mechanisms such as business/IT co-location, partnership rewards and incentives, shared understanding of business/IT objectives, cross-functional business/IT training, and cross-functional business/IT job rotation are of primordial importance. Enterprise Governance of IT structures and processes may be in place but when IT and business professionals do not understand each other and do not share the business/IT-related problems, a successful alignment between both areas will not be achieved. Implementing the right relational mechanisms will be the crucial enabler for better governance structures and processes (operational excellence perspective), higher stakeholders' satisfaction (stakeholder perspective), and ultimately a higher governance performance (corporate contribution perspective). Figure 7.6 displays the two distinct objectives of the future orientation perspective: skills and knowledge and IT/business partnership.

Within the **skills and knowledge** area, the cross-functional education and training metrics are predominant: *number and level of cross-functional business/IT training sessions*, *number of overall Enterprise Governance of IT training sessions*, *percentage Enterprise Governance of IT education per skill type*. A specific and important measure is the *number of Enterprise Governance of IT presentations for CEO and board members* capturing the communication efforts between the IT management team and its business hierarchy. *Level and use of Enterprise Governance of IT knowledge management system* refers to an intranet that all employees can access for seeking and sharing knowledge on the *Enterprise Governance of IT* practices within the organization.

IT/business partnership objectives report on the IT and business literacy of respectively senior business managers (*percentage of senior manager IT literate*) and the IT team (*percentage of IT managers business literate*). The importance of these two metrics is confirmed by Teo and Ang's study where the knowledge ability of IT management and top executives concerning business and IT were found to be two crucial critical success factors in business/IT planning alignment. *Level of business perception of IT value* can be measured through scores indicating the level going from 1 (perceived as a cost) to 5 (IT seen as a driver/enabler).

The performance of the Enterprise Governance of IT project can be visualized using this generic Enterprise Governance of IT BSC. The corporate contribution perspective of this scorecard matches with the IT function's balance scorecard (see Chap. 4). Indeed, the ultimate goal for both scorecards is to obtain better corporate financial results. The main difference between both scorecards is that the other perspectives focus completely on the Enterprise Governance of IT project. Some of the metrics of the Enterprise Governance of IT BSC will however be rolled-up and/or aggregated in the IT BSC, and vice versa. Additionally, the board BSC will certainly import some relevant Enterprise Governance of IT measures.

Improving the Enterprise Governance of IT performance is the main reason for building and implementing an Enterprise Governance of IT scorecard. It must be clear that just measuring is not enough; the scorecard must be implemented as a management system. When the measurements indicate that there are major problems with risk management (corporate contribution), a possible strategy may involve the improvement of the disaster recovery planning (DRP) through a COBIT implementation (operational excellence), which in turn may need a cross-sectional business/IT training in COBIT and DRP (future orientation).

Assignment Box 7.1: Improve the Enterprise Governance of IT BSC

Review the proposed IT governance BSC and improve it based on your insights of COBIT 5 enablers and processes.

Summary

There is no real “silver bullet” (the ideal way) for implementing and maintaining effective Enterprise Governance of IT within an organization. And in many cases, the key question is: how do you get started? This chapter provided some key success factors as demonstrated in other best practice cases and discusses external trigger events such as legal compliance or internal trigger events such a burning platform. To initiate and manage an enterprise governance improvement programmes, a BSC is outlined specifically in the context of enterprise governance of IT. It is clear that the ultimate expected contribution measured in such a scorecard is keyed around achieving alignment and business benefits out of IT-enabled investments.

Study Questions

1. Discuss some key success factors that can help in successfully introducing enterprise governance of IT.
2. Illustrate some pain points or trigger events that can act as burning platforms to initiate an enterprise governance of IT improvement programme.
3. Explain the four perspectives of the Enterprise Governance of IT BSC: corporate contribution, stakeholders, operational excellence, and future orientation.
4. Define and discuss typical metrics for each of the perspectives of the Enterprise Governance of IT BSC.
5. Explain the difference between an IT BSC and an Enterprise Governance of IT BSC.

References

- De Haes, S., Gemke, D., Thorp, J., & Van Grembergen, W. (2011). KLM's enterprise governance of IT journey: From managing IT costs to managing business value. *MISQ Executive*, 10(3), 109–120.
- Epstein, M. J., & Roy, M. -J. (2004, February). How does your board rate? *Strategic Finance*, 25–31.
- ISACA. (2012). *COBIT 5 Implementation*. Retrieved from www.isaca.org
- ITGI. (2003). *Board briefing on IT governance* (2nd ed.). Retrieved from www.itgi.org

Index

A

- Activity based costing, 14, 17, 26
- Alignment, 1–9, 14, 16, 18, 20, 29–31, 33–35, 37, 42, 45–69, 71, 80, 86, 88–89, 92, 98, 99, 103–106, 114, 121, 122, 126, 154–156, 159, 161, 162
- Applications, 3, 8, 16, 18, 22, 24, 36, 41, 42, 72, 79–82, 85, 86, 90, 91, 97, 112, 113, 121, 126, 138, 141, 147, 148, 153, 157, 158
- Architecture, 14, 16, 20, 26, 34, 36, 39, 41, 47, 48, 51, 59–61, 63–66, 68, 86, 88, 91, 92, 94, 95, 99, 111, 112, 121, 124, 145, 156
- Architecture steering committee, 14, 16

B

- Behavior, 3, 5, 11, 13, 58, 59, 113, 136, 145
- Benchmark, 50–52, 54, 55, 71, 80, 88, 90, 92–96, 126, 127
- Benefit, 7, 17, 26, 29–31, 33, 37, 71, 73, 78–79, 86, 99, 120–121, 124, 125, 151, 153, 162
- Benefits management, 14, 17
- Board of directors, 12–14, 16, 32, 34, 56, 87, 88, 114, 131, 140, 157
- Business case, 12, 14, 16, 24–27, 37, 71–79, 92, 99, 122–124, 148, 152
- Business Case Development, 78
- Business Case Maintenance, 77–78
- Business Case Review, 78
- Business case template, 27, 77, 124, 152
- Business/IT account management, 14, 17

C

- Charge back, 14, 17, 90
- Chief executive officer (CEO), 3, 13, 14, 16, 19–21, 24, 33, 51, 52, 117, 154, 157, 161
- Chief Information Officer (CIO), 3, 4, 12–14, 16, 17, 19–27, 29, 30, 33, 35, 37, 51, 52, 86, 88, 98, 117, 152–154, 157–159
- CMM, 124
- COBIT. *See* Control Objectives for IT and related Technology (COBIT)
- Co-location, 14, 17, 161
- Competency, 51, 156
- Compliance, 14, 16, 32, 35, 87, 92, 94, 95, 106, 111, 114, 124, 132, 143, 154, 157, 158, 160, 162
- Continuity manager, 24
- Control design, 132, 141, 142, 146, 149
- Control Objectives for IT and related Technology (COBIT), 3, 4, 14, 17, 32, 52, 94, 103–127, 129–149, 158, 159, 162
- Corporate contribution, 16, 81–83, 88–92, 98, 154–156, 161, 162
- COSO/ERM, 14, 17
- CRM. *See* Customer relationship management (CRM)
- Cross-training, 14, 17, 51
- Culture, 12, 29, 31, 56–68, 113, 120, 126, 135, 136, 152
- Customer relationship management (CRM), 3, 22, 72

D

Digitized organization, 1–4, 8, 33
Disclosure, 33–35

E

EDM. *See* Evaluate—direct—monitor (EDM)
End-to-end, 4, 104, 106–110
Enterprise goals, 50, 52, 53, 105, 106, 107, 109, 117, 120, 140, 144
Enterprise Governance of IT, 1–9, 11–42, 54–56, 103–127, 151–162
Ethics, 113, 126, 135, 157
Evaluate—direct—monitor (EDM), 32, 114, 126
Executive committee, 16, 19, 24, 26, 28, 33, 37, 54, 92, 123
Expression barriers, 5
External audit, 130, 154

F

Framework, 3, 4, 6, 11–14, 17, 33–36, 38, 42, 56–62, 69, 90, 94, 103–127, 129–149, 159
Functional integration, 4, 5
Future orientation, 16, 80, 81, 83, 88, 89, 94–99, 155, 161, 162

H

Help desk, 81, 82
Holistic, 11, 42, 104, 113–114, 131

I

Implementation barriers, 5
Incident management, 98
Information, 1, 2, 4–8, 11, 14, 16, 20–23, 25, 26, 33, 35, 38, 40, 47, 48, 65, 72–74, 81, 83, 85, 86, 88, 89, 97, 103, 106, 117–123, 125, 126, 131, 135, 137, 139–143, 146, 149, 152, 154, 156

Information economics, 7, 14, 16, 47, 48, 82, 121, 156

Information Systems Audit and Control Association (ISACA), 3, 4, 33, 72, 73, 103, 104, 107–112, 114, 116–119, 123, 125, 126, 129, 134, 139, 141

Information technology (IT) assurance, 16, 129–149 audit, 103, 129, 148, 156, 157 audit committee, 14, 16

balanced scorecard, 14, 16, 81, 82, 84, 86,

86, 88, 97–99, 106, 113, 126, 158

black hole, 71–72, 99

budget, 14, 17, 19, 24, 29, 30, 35, 82, 83

budget control and reporting, 14, 17

cost, 7, 17, 24, 26, 27, 29, 87, 90, 153, 156

director, 12, 13, 16, 32, 56, 140

expertise, 12, 14, 16, 34

governance, 2–4, 12, 14–17, 20, 32–37,

39–42, 49, 54–56, 69, 86, 88, 98, 103,

104, 114, 126, 158–161

governance assurance, 17

governance function/officer, 14, 16

leadership, 12, 14, 17

management, 3, 5, 11, 17, 32, 33, 54, 92,

93, 97, 103, 113–115, 140, 145, 146,

148, 157, 161, 162

manager, 13, 54, 65, 156, 161, 162

project steering committee, 13, 14, 16

related goals, 52, 53, 105–109, 116, 120,

140, 144

savvy, 33, 109

security steering committee, 16, 35

steering committee, 11–14, 16, 35, 113,

158, 159

strategy, 3–5, 13, 14, 16, 20, 24, 45, 56, 88,

90, 97, 111, 148, 158, 159

strategy committee, 13, 16, 56,

158, 159

Internal audit, 87, 91, 92

Internal control, 17, 34, 111, 132

Inter-organizational governance of IT, 36

Intra-organizational governance of IT, 36–37

Investment criteria, 110, 121

ISACA. *See* Information Systems Audit and Control Association (ISACA)

ISO, 3, 32, 115, 123

ISO/IEC 38500, 32, 114

ITIL, 112, 119

J

Job-rotation, 12, 14, 17, 161

K

Key performance indicators, 48

KLM, 4, 19–31, 34, 36, 37, 41, 42, 151–153

Knowledge management, 17, 94, 96, 161

L

Lag indicator, 81

Lead indicator, 81

M

Matching approach, 45, 46
Mirror roles, 23, 24
Moderation approach, 45–46

O

Operating effectiveness, 132, 142, 146, 149
Operational excellence, 16, 80–83, 88,
 89, 93–94, 98, 154, 155, 158, 159,
 161, 162
Outcome measure, 81, 98, 106, 115, 116
Outsourcing, 18, 23, 35, 48, 113, 153

P

Performance driver, 81, 98, 116
Performance management, 8, 34, 35,
 111, 154, 156
PMBOK, 112
Policy, 36, 41, 124, 140
Portfolio management, 11–16, 20, 21, 26–28,
 30, 31, 37, 39, 41, 111, 122–123, 152
Prince 2, 112
Process, 2–6, 8, 11–13, 15–22, 26–28, 30–38,
 41, 42, 51, 55, 56, 59, 67, 71–81, 85,
 87, 89, 93–94, 94, 96, 98, 99, 103, 104,
 106, 108–126, 129–133, 139–149, 152,
 154–162
 capability, 123–125
 maturity, 94, 95, 98, 123–125, 158, 159
 owner, 93, 94, 141
Profile deviation approach, 47
Project management, 139, 142

R

RACI chart. *See* Responsible, accountable,
 consulted, and informed (RACI) chart
Regulation, 34, 35, 57, 106, 157, 158
Relational mechanisms, 3, 11–13, 17–19,
 31, 36, 42, 55, 56, 113, 154, 155,
 159, 161
Responsible, accountable, consulted, and
 informed (RACI) chart, 109–110, 115,
 117–118, 141, 142, 146
Risk appetite, 110
RISKIT, 4, 104, 110–112
Risk management, 1, 4, 8, 34, 35, 88, 91, 92,
 98, 104, 124, 139, 156, 157, 162

S

SAM. *See* Strategic alignment model (SAM)
Scope, 18, 59–61, 63–66, 68, 77, 92,
 112, 120, 124, 139, 140, 144, 145,
 156, 157

Scoring approach, 47–50
Security/compliance/risk officer, 14, 16
Security manager, 139
Service level agreements, 14, 17, 51,
 110, 119

Service manager, 24

Services, 1, 7, 8, 11, 17–20, 22–26, 29,
 34, 36, 39, 41, 48, 50, 51, 54, 55, 65,
 77, 79, 80, 83–93, 97, 98, 110–113,
 115–117, 119, 120, 126, 138, 145, 146,
 148, 153, 157

Skills, 51, 59–61, 63, 65, 66, 68, 94, 113, 139,
 140, 153, 156, 161

Specification barriers, 5

Strategic alignment model (SAM),
 4–6, 159

Strategic fit, 4

Strategic information systems
 planning, 14, 16

Structures, 2–4, 8, 11–13, 18, 19, 28, 31, 33,
 36, 38, 41, 42, 51, 55, 56, 80, 85, 113,
 115, 125, 126, 129–131, 140, 141, 149,
 154, 158, 159, 161

T

Testing, 28, 139–144, 146–148

TOGAF, 112

Transparency, 18, 35, 51, 58, 59, 93, 110, 135,
 145, 152, 158

U

User orientation, 16, 80, 82

V

VALIT, 72, 104, 110–112

Value, 1–9, 16, 20–22, 27–29, 31, 34–38, 47,
 48, 50, 51, 58–66, 71–73, 77, 79–81,
 86, 88, 89, 92, 93, 97–99, 104–106,
 109, 110, 113, 120, 124, 145, 151–156,
 159, 161, 162

Value management office, 21, 28

Viable system, 11, 37–39