University of Applied Sciences and Arts Northwestern Switzerland
School of Business

IT Governance for SME

Thesis for the attainment of the academic degree of

Master of Science (MSc)

in

Business Information Systems

by Peter Josi (06-631-774)

Handed in: 31th July 2012

Supervisor: Prof. Dr. Rainer Telesko

***Abstract* — The usage of information technology (IT) has drastically emerged during the last decade. Often, IT is considered to be the backbone of all business processes and the demand regarding stable and flexible IT services is continuously increasing. Users want to have access to their information from everywhere and all the time. Small and medium-sized enterprises are facing the challenge to satisfy these demands. Due to restricted financial and personal resources that are disposable for IT, small and medium-sized enterprises are depending on solid and efficient IT processes in order to remain competitive.**

This is where IT governance comes into play. Simply put, the main objective of IT governance is to ensure that IT processes are optimally aligned to the business processes whilst running at the highest possible efficiency-level. Currently, IT governance is not yet widespread in small and medium-sized enterprises. The reason for this is, on the one hand, missing guidance for the implementation and management of IT governance processes. There are numerous frameworks and standards that are primarily appropriate for larger companies but none of them can be deployed in small and medium-sized enterprises due to their vast implementation effort that has to be taken. On the other hand, IT governance is considered to be a luxury topic from the perspective of many smaller companies and therefore does not get the necessary attention. The rethinking process that IT is a major enabler of business services has not yet advanced to the majority of small and medium sized enterprises.

The underlying hypothesis of this paper is that the existing IT governance frameworks and standards are not applicable for small and medium-sized enterprises and that there is a more effective way of how IT governance can be addressed. In this paper, an IT governance framework for small and medium-sized enterprises is presented.

Based on surveys and interviews, the specific requirements of small and medium-sized enterprises regarding IT governance are analysed which then serve as a basis for the design of the framework. The directives within the framework are taken out of the existing IT governance frameworks and tailored to the requirements identified during the surveys and interviews. This approach ensures that the specific expectations of small and medium-sized enterprises can be fulfilled by coincidentally remaining compatible and to rely on best practices.

Furthermore, a lifecycle is presented which helps small and medium sized enterprises during the implementation of the framework. The first step of the assessment is to assess the current situation. An online assessment which can be conducted at www.it-governance-for-sme.ch supports potential users to determine their IT governance maturity. Within the assessment, all relevant IT processes are addressed and the result of the assessment is then linked to the processes of the framework. The

assessment is a good starting point for any enterprise that wants to implement IT governance processes, regardless of whether they are planning to use this framework or not.

Testimonials by industry experts, a statement of applicability of a potential user and a listing of the benefits of using this framework complete this paper.

***Index Terms* — IT Governance, IT Management, SME, COBIT, Framework**

STATEMENT OF AUTHENTICITY

This paper includes about 21’000 words (chapter I to chapter VII) and I herewith confirm that the information presented herein is my own work. Whenever other sources are used, they are clearly mentioned in the text and listed in the bibliography.

I am informed about the fact that any plagiarized misleading content as well as not correctly stated sources will inevitably lead to the loss of the corresponding credits or degree related to this work.

I declare that all information and statements contained in this paper are fully correct to my best knowledge and belief.

Peter Josi

ACKNOWLEDGMENT

I would like to thank everyone who supported me on writing this paper. Firstly, I thank the participants of the survey and the interview partners who were willing to give me their time. These partners were, in alphabetical order:

- Bernasconi, Sandro (Bucher Hydraulics, Frutigen)
- Bosshard, Hugo (Studerus AG, Schwerzenbach)
- Fischer, Markus (Fischer-ICT GmbH, Adelboden)
- Schärz, Hans (Wandfluh AG, Frutigen)
- Schranz, Jonathan (Künzi & Knutti AG, Adelboden)
- Utiger, Christoph (Kambly SA, Konolfingen)
- Zurbrügg, Martin (Informaticon AG, Thun)

The design of the framework is heavily depending on the insights provided by the survey results and the interesting dialogues.

Secondly, another valuable input for the revision of the initial draft of the framework was delivered by Peter R. Bitterli (bitterly-consulting.ch) and Prof. Dr. Christian Thiel (University of Applied Sciences of St. Gallen). Nowadays, it is not a matter of course that these committed persons took the time to study the framework and to write meaningful testimonials. For the statement of applicability, Hugo Bosshard (Studerus AG, Schwerzenbach) who was already an interview partner consented to support me. Many thanks at this place for the testing and verification of the framework.

Further, thanks go to my supervisor, Prof. Dr. Rainer Telesko. He offered support in a very constructive way and accompanied me during the whole semester. It was a pleasure to work with Rainer.

Last but not least, one big thank you goes to my girlfriend and my family who supported me during the whole education.

TABLE OF CONTENT

I. Introduction

The usage of Information Technology in the daily business has become very important. Almost all companies have some kind of dependence regarding IT and thus, proper management of IT resources has become more important. Innovative and effective usage of IT resources may lead to significant competitive advantage. Even more, the emergence of IT has enabled new business models and has made business processes more flexible than ever. One might say that many companies would not be able to survive without IT and therefore it is very important to take serious care of IT.

The management of IT resources could be comprised under the term IT governance. The primary goal of IT governance is to align the business strategy and the business requirements with IT. There are several frameworks and standards that support companies across the whole lifecycle of the IT governance process. The ubiquity of IT not only affects large companies, hence IT governance is also very important for small and medium-sized enterprises. But due to the limited resources and the complexity of the whole topic, a holistic approach for managing and controlling IT resources has proven to be a major challenge for small and medium-sized enterprises. The key question is how IT governance methods and principles can be applied for small and medium-sized enterprises. The problem with existing frameworks and standards is that they are not suitable in size and scope for small and medium-sized enterprises and therefore have not found broad acceptance yet.

In this paper, an IT governance framework for small and medium-sized companies is presented. The first chapters provide a brief overview about the topic IT governance and dismantle the term to its components. In the following, a brief review of existing literature and research activities concerning the topic IT governance for small and medium-sized is presented. This chapter depicts the underlying motivation for writing this paper as there is currently no suitable IT governance framework for small and medium-sized enterprises available. To develop such a framework, it is vital to know the end-users requirements and expectations. In consequence of this fact, a research activity has been conducted to identify the needs of small and medium sized companies regarding IT governance. The setup and the results of the research process are presented in chapter IV.

The framework is designed with great influence of the research activities results and the already existing frameworks and standards. The structure of the framework is heavily depending on the identified requirements of small and medium-sized enterprises whereas the actual content of the framework orientates itself to the existing frameworks and standards. This mixture allows meeting the specific demands of small and medium-sized companies by simultaneously remaining compatible and compliant with the industry standards which can be considered as best practices. The main idea of the framework is to make the content of proved and established guidelines and standards accessible so that also small and medium-sized enterprises can profit from this experience. In order to reach this, the framework has to be tailored to the needs of small and medium-sized enterprises.

The hypothesis of this paper is that the existing IT governance frameworks and standards are not applicable for small and medium-sized enterprises and that there is a more effective way of how IT governance can be addressed. The hypothesis is tested on one hand by expert reviews and on the other hand, a statement of applicability of a potential end user. This testing approach ensures to make a qualitative assertion whether or not the framework meets the end users expectations. At the same time, the content-validity is examined.

II. What is IT Governance?

The governance of enterprise IT has become an important topic for many enterprises. Triggered by the financial crisis at the turn of the millennium, authorities fortified the laws and regulations regarding financial reporting and, in doing so, also tightened the measures for IT auditing and control. This intensification of regulation pursues the goal of transparent, responsible and comprehensive management and control of organizations and their alignment to regulations, standards and ethical policies, which was claimed by both, shareholders and stakeholders (Rüter, Schröder, & Göldner, 2006, p. 6). Therefore IT processes face the same regulations and have to fulfill them regarding transparency, integrity and compliance.

The impact for IT departments is severe because nowadays, business processes are highly automated with minimal interference of human operations. Frequently business transactions are executed with greatest assistance of information technology, meaning that changings of laws and regulations may impact the IT process and force the IT department to make adaptations. The requirement from the users that information has to be accessible everywhere and any time are even complicating the matter (Johannsen & Goeken, 2011, p. 8). This evolution is called the transformation from the industrialization to the digitalization and the formation of a digital native society. A study conducted by the IT Governance Institute (IT Governance Institute) in 2008 confirms this development. In the study, 93 percent from totally 749 asked executives stated that IT captures a significant role. The study also unveiled that 36 percent admitted that the IT strategy was not aligned to the corporate strategy. The results of this study clearly unveil an imbalance between the perceived importance of IT within the enterprise and the attention that IT becomes from the board of executives, especially regarding strategic alignment. Solid IT governance helps to improve this disparity by governing the business requirements that the business has against it and ensuring effective and efficient operations (IT Governance Institute & KPMG, 2003, p. 26).

This chapter provides an overview about the topic IT governance. First, different definition approaches from several standardization bodies or institutions are presented and interpreted. Second, IT governance is divided in its core elements which are briefly explained.

1. Definition

Corporate governance is the umbrella term of all governance activities in the whole enterprise. The term is defined by the OECD as follows (Organisation for Economic Co-operation and Development, 2004, p. 11):

“*Corporate governance involves a set of relationships between a company’s management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring.*”

According to the definition, corporate governance signifies to reliable and long-term added value that is observed through monitoring and controlling mechanisms. It is considered to be a top-management topic, involving also stakeholders and shareholders. The main goal of corporate governance is to improve transparency within and beyond company boarders.

Figure 1 illustrates the various impact factors and the involved stakeholders. Important to notice is that corporate governance is mainly driven by external factors and, with regard to IT governance, has great impact to IT operations. IT governance in this context functions as some kind of intermediary by aligning the demand of the corporate governance side with the internal requirements of the IT.

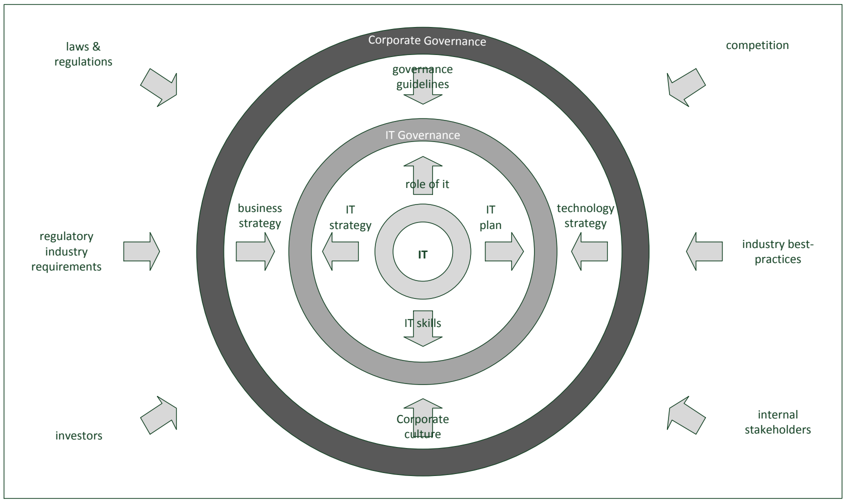


Figure 1: Reference frame for IT governance, following (Rüter, Schröder, & Göldner, 2006, p. 11).

The depicted figure clearly indicates the relation between corporate governance and IT governance. However, it is still not defined whether IT governance is a discrete subdomain of corporate governance or it should be treated within the cloak of corporate governance. There are also other departments where governance activities should be in place, like human resources governance or engineering governance. There are votes that endorse that IT governance takes some kind of privileged position as a discrete subdomain but there are also votes who argue that IT governance should be embedded in corporate governance (IT Governance Institute, 2009, p. 10).

Current research activities and the various existing frameworks mainly treat IT governance as a discrete subdomain but tightly aligned with the enterprise's corporate governance. The argumentation is the fact that information has become the most important factor of production and should therefore be treated with special attention (Rüter, Schröder, & Göldner, 2006, p. 15).

Up to now, there is no common agreed definition upon the term IT governance. In the Cadbury Report (Committee on the Financial Aspects of Corporate Governance, 1992), IT governance is defined as a

"system by which companies are directed and controlled"

Adrian Cadbury chairs a committee for mitigating corporate governance risks and failures whose results are published in the Cadbury Report. The Cadbury Report contains one of the oldest definitions of IT governance. The definition does not distinguish between IT and non-IT and has strong similarity to the corporate governance definition of the OECD. Another definition was developed by the IT Governance Institute (IT Governance Institute, 2003, p. 19):

"IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."

Continuous alignment between business and IT is the main statement of this definition. IT governance is considered to be a part of corporate governance (or above called enterprise governance) and the IT Governance Institute clearly assigns the responsibility to the top-level management.

The definition of Weill and Ross from the MIT Sloan School of Management Center for Information System Research (CISR) is as follows (Weill & Ross, IT Governance - How Top Performers Manage IT Decision Rights for Superior Results, 2004, p. 8):

"IT Governance: specifying the decision rights and accountability framework to encourage desirable behavior in using it."

In the definition of Weill and Ross, decision rights and responsibilities are treated to be the main components of an IT governance framework. The concrete reference to a framework is unique in this definition. A framework in this context is considered to be a set of principles dedicated to determine the accountability within IT. In Figure 2, Weill and Ross describe the relationship between corporate governance and IT governance.

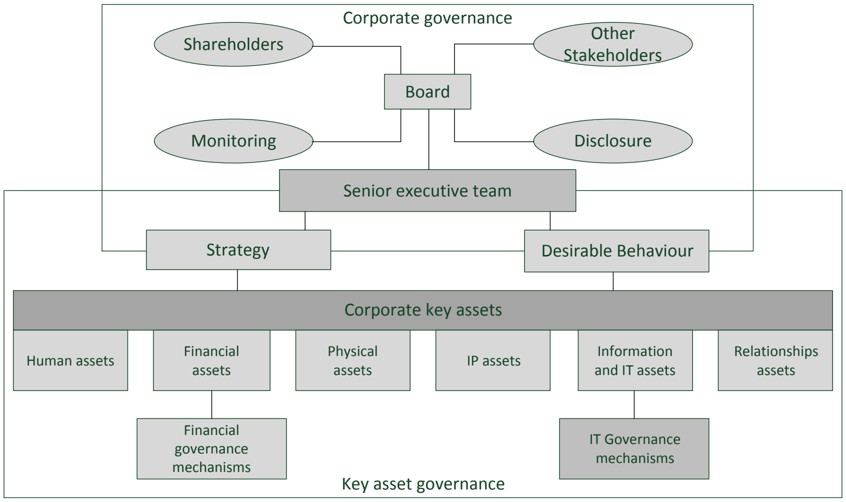


Figure 2: Corporate and key asset governance, following (Weill P. , 2004, p. 5).

The figure shows that, because strategic alignment is crucial to the business success, IT governance cannot be separated from corporate governance activities.

A rather stronger emphasis of the importance of the relationship between business and IT can be found in the definition of De Haes / van Grembergen (De Haes & van Grembergen, 2004):

"IT Governance is the 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"

To summarize organizational structures and management and control processes is a core element of IT governance. The responsibility to govern IT is not within the IT department but is assigned to the board of directors, emphasizing that IT governance cannot be considered in isolation but has a strong relationship to corporate governance activities. What is missing in all of the above mentioned definitions are means to implement effective and efficient IT governance. There is also no common agreed model or framework for IT governance. A review to the history of IT governance explains why until now no standard could be agreed upon.

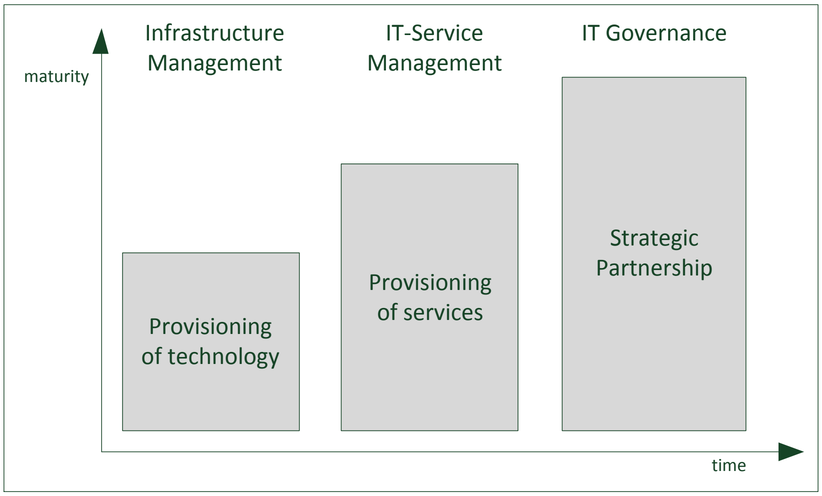


Figure 3: Evolution of IT governance, following (Bensch, 2006, p. 24).

At the early stage, the provisioning of technology, called infrastructure management, was the core business of the IT departments. As IT became more and more complex and the demands in availability increased and IT was considered to be a service provider. From this point, IT was no longer only operator of the infrastructure but had to take care about whole business applications. This was an important shift because IT was then involved in business processes and the business departments nowadays have to share their knowledge with IT staff. Johannsen (2011, p. 9) believes that in future, the importance of IT will increase but due to the ongoing standardization and homogenization, IT will more be considered as a commodity by referring the prominent article form Nicolas Carr – “IT doesn’t matter” (Carr, 2003). In this future state, IT governance will take greater significance than ever.

2. IT Governance Focus Areas

Accomplishment of business value and minimization of IT risk are the main IT governance goals, according to the IT Governance Institute (IT Governance Institute & KPMG, 2003). In order to fulfill these goals, the stakeholder value drivers should primarily be taken into account and mapped to the enterprise goals (strategic alignment). Additional IT value can best be realized by considering the enterprise goals that determine the IT goals. Proper risk management leads to a minimization of IT risk and a better fulfillment of the IT goals, which should be measured on a regular basis. This IT governance process is depicted in Figure 4.

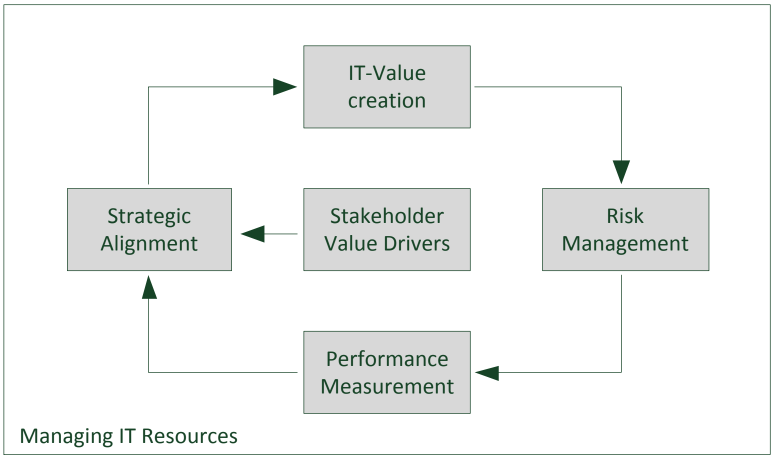


Figure 4: Focus of IT governance, following (IT Governance Institute & KPMG, 2003, p. 27).

Together with leading analysts like Gartner and KPMG, the IT Governance Institute (ITGI) has defined five IT governance focus areas (see Figure 5).

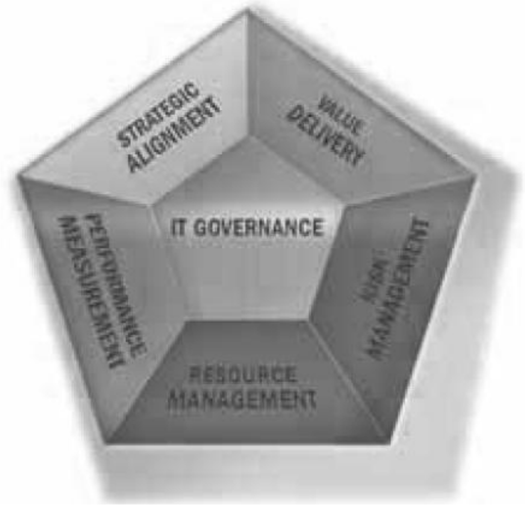


Figure 5: IT governance focus areas (ISACA, 2007, p. 6).

2.1 Strategic Alignment

The primary goal of strategic alignment is to align priorities, competences, decisions and activities of IT with the business (Johannsen & Goeken, 2011, p. 14). This goal has proven very hard to deal with because of the various interdependencies between business and IT. There are also discussions whether or not technology should follow strategy or vice versa (Pfeifer, 2003). Technology may be a strong enabler for the business but it does not always mean that new technology is better.

This mutual dependence between business and IT has aroused several alignment models, among which the Strategic Alignment Model (SAM) from Henderson & Venkatraman (1989) is the most popular. The SAM confronts the business with IT on both, a strategic and an infrastructure level. It is composed of four domains with each three components and contains linkages between any domain (strategic fit and functional integration).

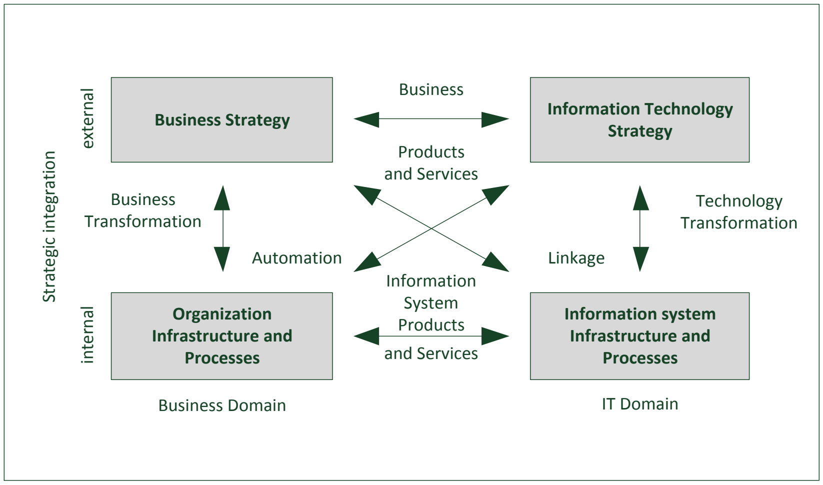

Strategic integration
external
internal
Business Strategy
Information Technology Strategy
Business
Products and Services
Business Transformation
Technology Transformation
Automation
Linkage
Information System Products
and Services
Organization Infrastructure and Processes
Information system Infrastructure and Processes
Business Domain
IT Domain

Figure 6: Strategic Alignment Model, following (Macdonald, 1994).

Strategic fit indicates the vertical alignment between the strategy and the infrastructure domain, the functional integration labels the horizontal alignment. According to Henderson & Venkatraman, alignment in this context means “a balance among the choices made across all four domains” (Henderson & Venkatraman, 1989, p. 477) . Important hereby is that multilateral, not bilateral alignment is determining. The SAM is used as a structural help and a model to systematically analyze an alignment problem, however on a highly abstract and theoretical level.

2.2 Value Delivery

IT departments should no longer be considered as a cost factor but as a supplier of true economic value. Therefore it is inevitable to associate IT with business processes and the company's goals (Holtschke, Heier, & Hummel, 2009, p. 1). But what is value? The IT Governance Institute defines the term value as follows:

Value is defined as the total life-cycle benefits net of related costs, adjusted for risk and (in the case of financial value) for the time value of money. (ISACA, 2008, p. 10)

True value from IT is generated when IT services are provided in the right quality, the right time and within the given budget. Proper IT service management can bring along competitive advantage, increase customer satisfaction and profitability. The IT department should also take a proactive role in value delivery. Not only should they take action when new investments have to be done. As a value driver, the IT has the burden to recognize potentials and to push them.

The following picture shows the coherence of value delivery. Attention should be paid to the fact that IT has no direct impact on the value production. It is difficult to quantify the value that IT generates because some elements can only be measured from a sentimental point of view.

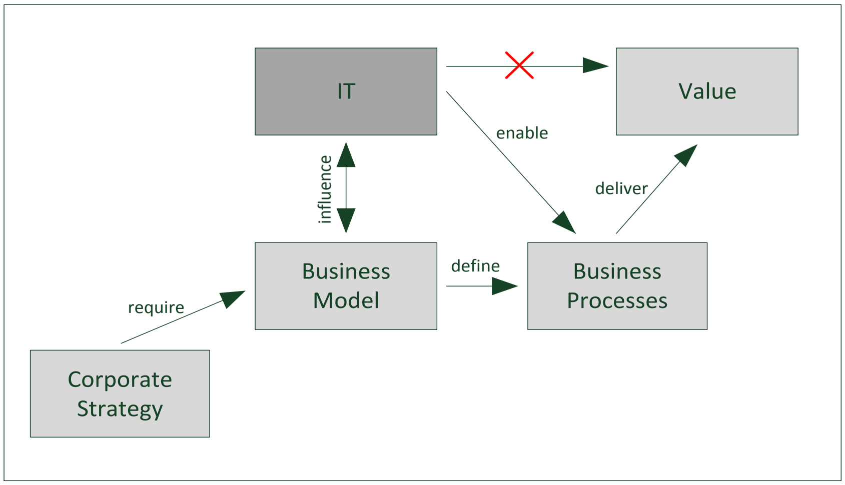


Figure 7: Contribution of IT to business success, following (Kremar, 2004, p. 399).

2.3 Risk Management

Information has become crucial for business success and the use of IT has opened great chances but also took along significant risks (Landolt, 2009, p. 22). These risks may not affect the business and therefore, IT related risks have to be carefully treated. To identify threats, usually a threat analysis is done which is then transformed to a weak spots analysis. The goal of a proper risk management is to minimize the IT related risk and to eliminate every unpredictable risk. It is then the responsibility of the higher management to decide whether to take the risk or not, depending on the respective risk appetite of the company. Risks are usually scaled into categories depending on the potential height of the damage and the probability of occurrence. Figure 8 shows such a classification scheme provided by Heinrich & Lehner.

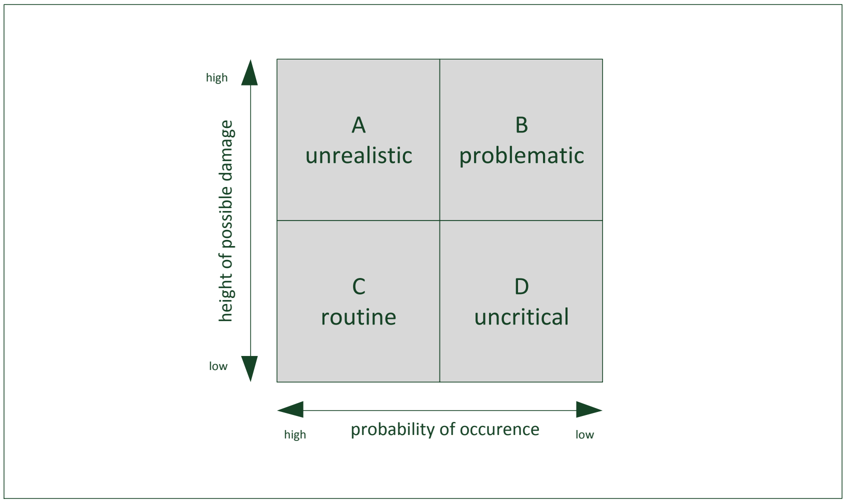


Figure 8: Risk classification, following (Heinrich & Lehner, 2005).

According to the risk category, the management then has to decide how to encounter the risk. Typically, there are three ways (IT Governance Institute & KPMG, 2003, p. 37)

- Risk reduction – Implement controls
- Risk transfer – Outsourcing, insurance
- Risk acceptance – Risk is officially recognized

2.4 Resource Management

Managing IT resources is an important part of IT since the continuous advancement and the many changes IT encounters. Successful management of IT resources requires deliberate decisions of the IT management (Lindstöm, Gammelgard, Simonsson, & Jonsson, 2005). IT resource management can be split up in the following key factors (IT Governance Institute & KPMG, 2003, p. 38):

- Human Resources – internal and external employees, consultants and specialists
- Applications – operating systems, application software and databases
- Technology- hardware, peripheral devices
- Facilities – buildings, technical equipment, power and supplies
- Data – stored information and knowledge

In order to succeed in IT resource management, the following factors have to be fulfilled. First, the responsibility must be clear for the management of IT systems and the management has decided for the right it services and suppliers. Then, IT staff is well qualified concerning the management of the IT infrastructure as well as IT projects. There has also to exist sensible planning activities such as budgeting, staff training and development. It is always a matter of resources when new projects have to be compared relating to their benefit, profitability and urgency.

IT portfolio management is a way to manage resources by constantly assessing the current activities or upcoming projects. It has significant impact when it comes to the identification, selection, prioritization and resource allocation for queuing projects.

IT portfolio management brings the following benefits (Cubeles-Marquez, 2008, p. 33):

- maximization of the return on investment (ROI) of IT projects
- transparency within the selection process of IT projects
- consolidation of projects and prevention of multilane activities through a central overview
- efficiency in IT resource management
- standardized measurement and reporting

2.5 Performance Measurement

IT is considered to be an enabler for increase in efficiency in all processes of an enterprise. On the other hand, IT has to work efficient, flexible and economic and these mutual requirements are sometimes hard to satisfy. The goal of IT performance measurement is to track the IT department in respect of cost, performance and business value (Johannsen & Goeken, 2011, p. 11). IT performance measurement eases to make qualified statements about the capability of the IT and therefore enables comparisons across company boarders. IT performance measurement is not self-purpose although does not create any direct business value. It is to a greater degree an analysis and control instrument of the other IT focus areas by screening them and making the information available to the IT management (IT Governance Institute & KPMG, 2003, p. 40).

The Balanced Scorecard (BSC) approach from Kaplan and Norton (Kaplan & Norton, 1992) is widely used in the industry and has become a tried and tested method also for IT performance measurement. The Balanced Scorecard has been published in 1992 in the Harvard Business Review. It is a strategic performance management tool that enriches the pure financial perspective with three further strategic components.

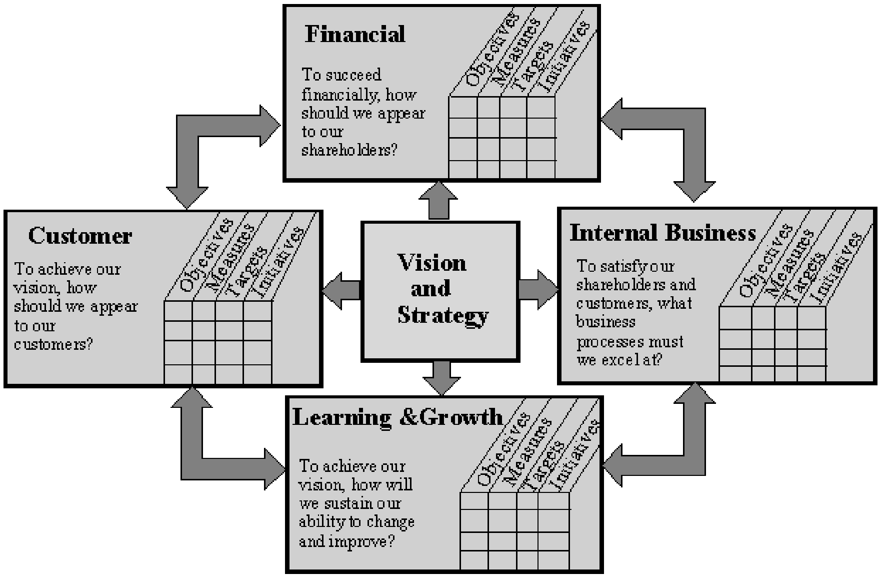

Financial
To succeed financially, how should we appear to our shareholders?
Objectives
Measures
Targets
Initiatives
Customer
To achieve our vision, how should we appear to our customers?
Vision and Strategy
Internal Business
To satisfy our shareholders and customers, what business processes must we excel at?
Learning &Growth
To achieve our vision, how will we sustain our ability to change and improve?

Figure 9: The balanced Scorecard (Martin, 2012).

The financial perspective still remains an important domain unlike other reporting methodologies, but extended with a customer-, an internal processes- and learning and growth perspective the BSC provides a holistic view about the whole enterprise. It also encourages recognizing relationships among the different perspectives. For each perspective, objectives, measures, targets and initiatives have to be defined. The quantity of key figures is depending on the size of the company.

The BSC can only be applied for IT if the original perspectives become adapted to the IT environment. The usage of an IT BSC is an effective means to help decision makers to align IT to the business requirements.

By reading the BSC, the management often fails to recognize the coherence between the perspectives (Bea & Hass, 2005, p. 202). Therefore, an additional step has to be done which considers the cause and effect relationship between the different perspectives and figures. Figure 10 shows the cause and effect between the IT BSC perspectives.

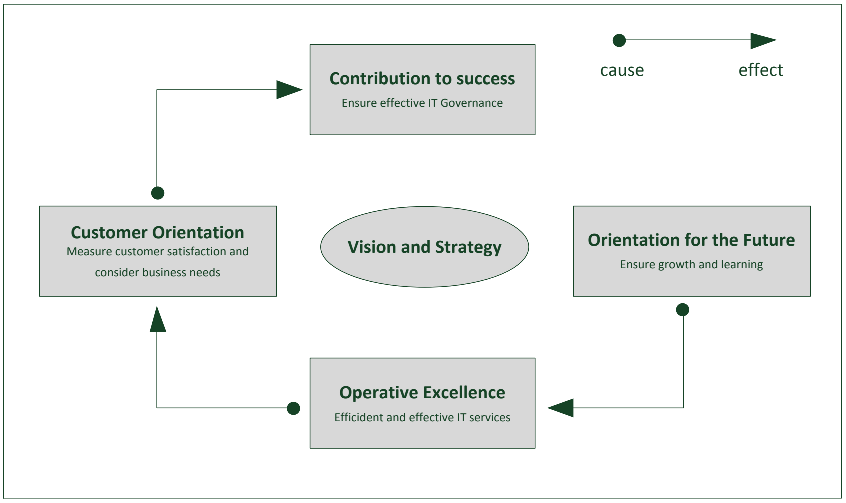

cause
effect
Contribution to success
Ensure effective IT Governance
Customer Orientation
Measure customer satisfaction and consider business needs
Vision and Strategy
Orientation for the Future
Ensure growth and learning
Operative Excellence
Efficident and effective IT services

Figure 10: Cause and effect betw. IT-BSC principles (IT Governance Institute & KPMG, 2003, p. 43)

3. IT Governance Frameworks

In this chapter, the framework COBIT 5 and the standard ISO/IEC 38500 are introduced. The goal of this chapter is to provide a brief overview of each, to describe its main purpose and to mention its practical importance and its propagation.

3.1 COBIT 5

COBIT is the most well-known framework for IT governance. COBIT was announced in 1993 by the Information Systems Audit and Control Association (ISACA). The current edition is COBIT 5 (ISACA, 2012) which was released in April 2012

COBIT has its nature in audit and control and was priory developed for the internal and external auditors revising the company's financial department. With the increasing impact of IT, the need for stronger governance of IT resources arose and COBIT expanded its focus by taking into account the requirements of the internal IT staff for IT management. In COBIT 5, information is considered to be the key factor of production and information technology is a major enabler to create, use, retain, disclose and destroy information. The COBIT 5 Executive Summary (ISACA, 2012, p. 3) enlists the following benefits that information and technology brings to the business:

- Maintain quality information to support business decisions.
- Generate business value from IT-enabled investments, i.e., achieve strategic goals and realize business benefits through effective and innovative use of IT.
- Achieve operational excellence through reliable and efficient application of technology.
- Maintain IT-related risk at an acceptable level.
- Optimize the cost of IT services and technology.

The application of COBIT 5 within an enterprise supports to realize these benefits through effective governance and management of enterprise IT. To summarize, COBIT 5 helps enterprises to get optimal value from their IT by "maintaining a balance between realizing benefits and optimizing risk levels and resource use" (ISACA, 2012, p. 5). COBIT 5 is based on 5 key principles for governance and management of enterprise IT.

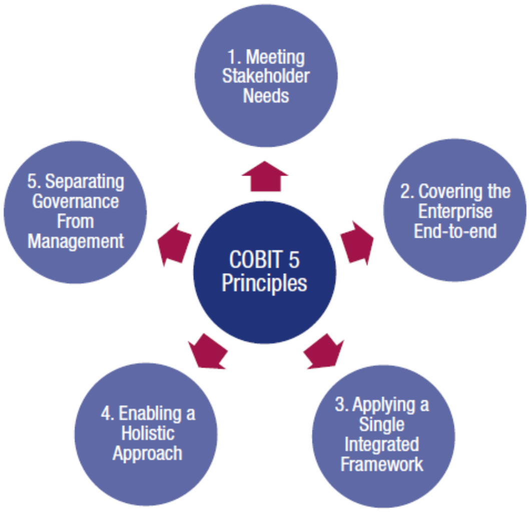

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Figure 11: COBIT 5 principles (ISACA, 2012, p. 13)

According to COBIT 5, value creation is the top governance objective for any enterprise in order to satisfy the stakeholder needs. Value creation means realizing benefits at an optimal resource cost whilst optimizing risk. To realize these benefits, it is recommended to consider all aspects relating to information technology and to apply a single framework that integrates all relevant standards or other frameworks. All governance activities should be tracked from a business perspective to ensure a holistic view. For proper management of IT, COBIT 5 makes a clear distinction between governance and management processes.

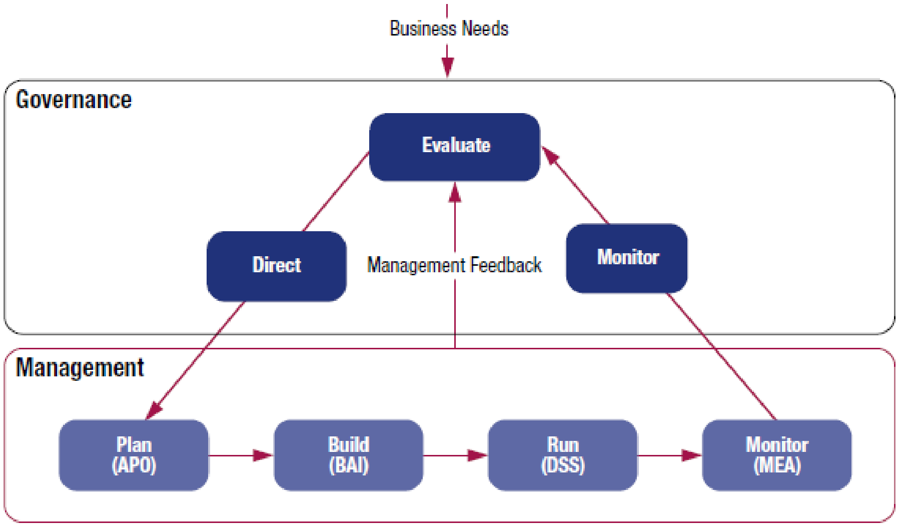


Figure 12: COBIT 5 governance and management key areas (ISACA, 2012, p. 32)

Governance processes ensure that enterprise objectives are achieved whereas management processes ensure efficient and effective implementation of IT processes according to the governance body. COBIT 5 contains five governance respectively management areas and 37 processes. Each process contains a description and a purpose statement. For the linkage between IT goals and business goals, a table is provided that also enlists the relevant metrics. Furthermore, each process contains a RACI chart. The most important parts of each process are the enlisted governance respectively management practices. These practices describe the activities that should be implemented. The following figure depicts the structure of the COBIT 5 framework.

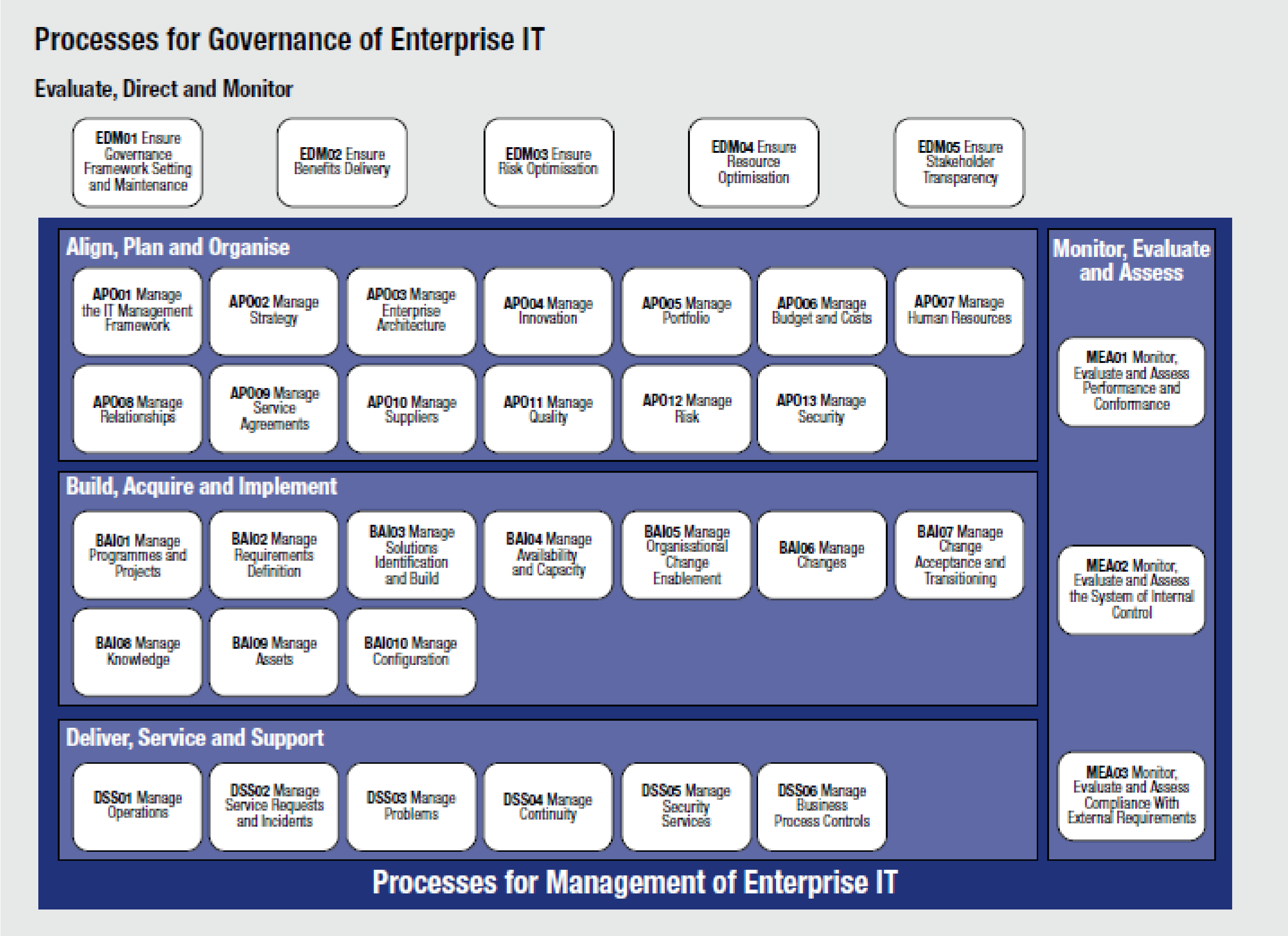

Processes for Governance of Enterprise IT
Evaluate, Direct and Monitor
EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency
Align, Plan and Organise
APO01 Manage 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
Build, Acquire and Implement
BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BAI03 Manage Solutions Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organisational Change Enablement
BAI06 Manage Changes
BAI07 Manage Change Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI010 Manage Configuration
Deliver, Service and Support
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
Monitor, Evaluate and Assess
MEA01 Monitor, Evaluate and Assess Performance and Conformance
MEA02 Monitor, Evaluate and Assess the System of Internal Control
MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Processes for Management of Enterprise IT

Figure 13: COBIT 5 process reference model (ISACA, 2012, p. 33)

The following picture illustrates the related standards that were considered and are integrated in COBIT 5. COBIT 5 integrates other IT relevant frameworks into one single framework. COBIT 5 can be considered to be some kind of umbrella framework that defines all IT processes. The respective execution of the processes is described in COBIT 5, however with linkage to other specialized frameworks for the actual topic.

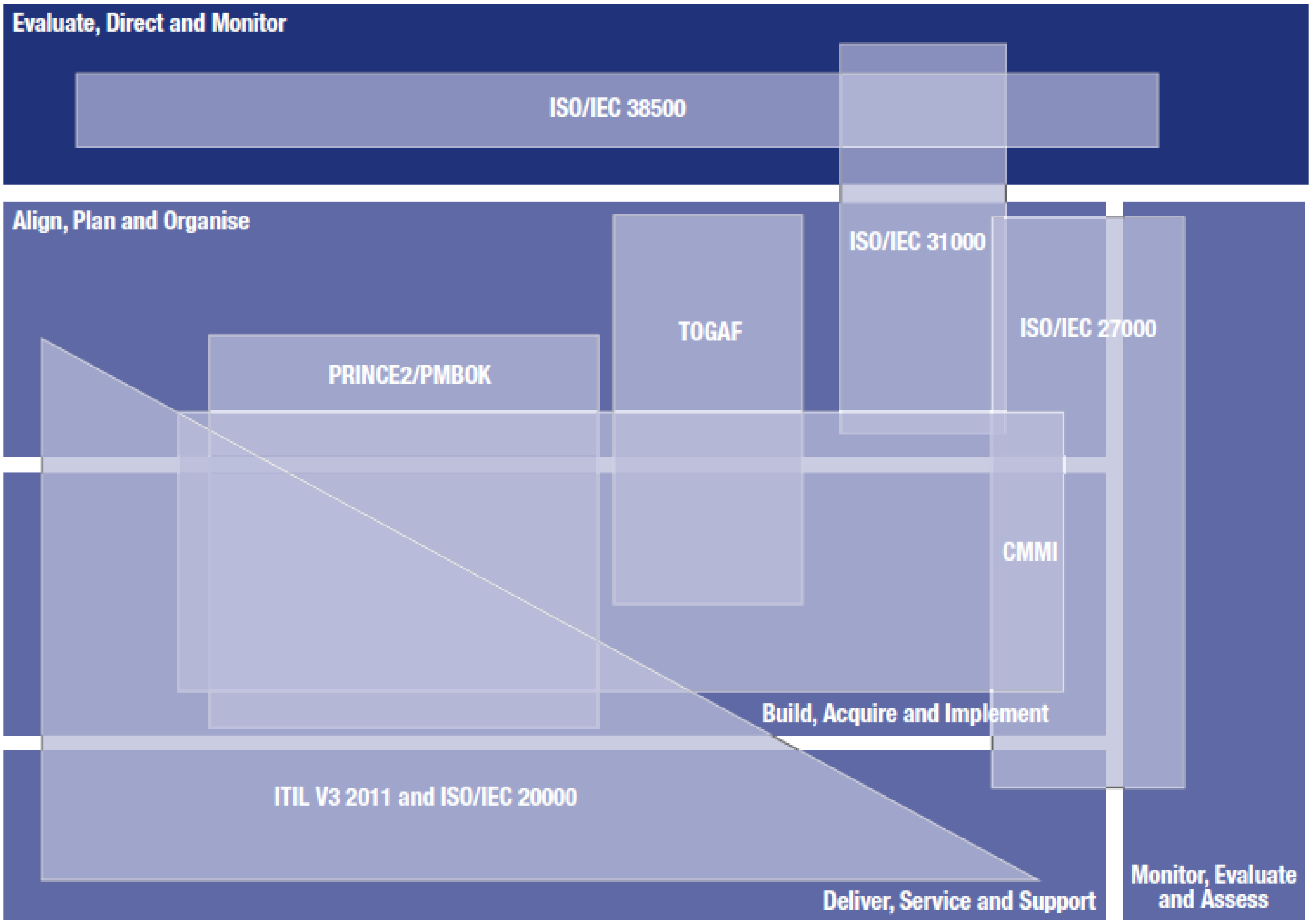

Evaluate, Direct and Monitor
ISO/IEC 38500
Align, Plan and Organise
TOGAF
ISO/IEC 31000
ISO/IEC 27000
PRINCE2/PMBOK
CMMI
Build, Acquire and Implement
ITIL V3 2011 and ISO/IEC 20000
Deliver, Service and Support
Monitor, Evaluate and Assess

Figure 14: COBIT 5 coverage of other standards and frameworks (ISACA, 2012, p. 61)

An introduction in all of the above mentioned standards and frameworks would extend the scope of this paper. Important to notice is that COBIT 5 should be considered in isolation but furthermore as an integrator framework that tries to bring together these different standards and frameworks and to consolidate them within one single framework tailored to the needs of the respective company.

3.2 ISO/IEC 38500

The standard ISO/IEC 38500 – Corporate Governance of IT (International Organization for Standardization, 2008) was published in 2008 by the International Standardization Organization. Although ISO 38500 has not fount broad coverage yet, it provides an internationally accepted basement upon definitions and best-practices in the area of IT governance. According to Figure 15, ISO/IEC 38500 is the only standard dedicated to only IT governance topics and this is the reason why this standard is briefly introduced in this paper.

ISO 38500 can be considered as a high-level standard due to its level of detail and is mainly addressing the higher management. The ISO 38500 standard is divided into two components, principles and a model for corporate governance of IT. There are six principles and which should ensure good corporate governance of IT. The responsibility to their application is at the director's level.

Responsibility	Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.
Strategy	The organization's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy.
Acquisition	IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.
Performance	IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.
Compliance/Conformance	IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.
Human Behavior	IT policies, practices and decisions demonstrate respect for Human Behavior, including the current and evolving needs of all the 'people in the process'.

Table 1: ISO/IEC 38500 principles (ISO 2008, p 9 - 15).

Every principle is then applied in a control circuit consisting of the three tasks evaluate, direct and monitor. Compared to COBIT, there are not many similarities which show that the field of IT governance is still in its infancy (Johannsen & Goeken, 2011, p. 195). One thing they have in common since the newest version of COBIT is the governance cycle evaluate, direct and monitor. This development may be the beginning of the harmonization of the existing frameworks which is an important step.

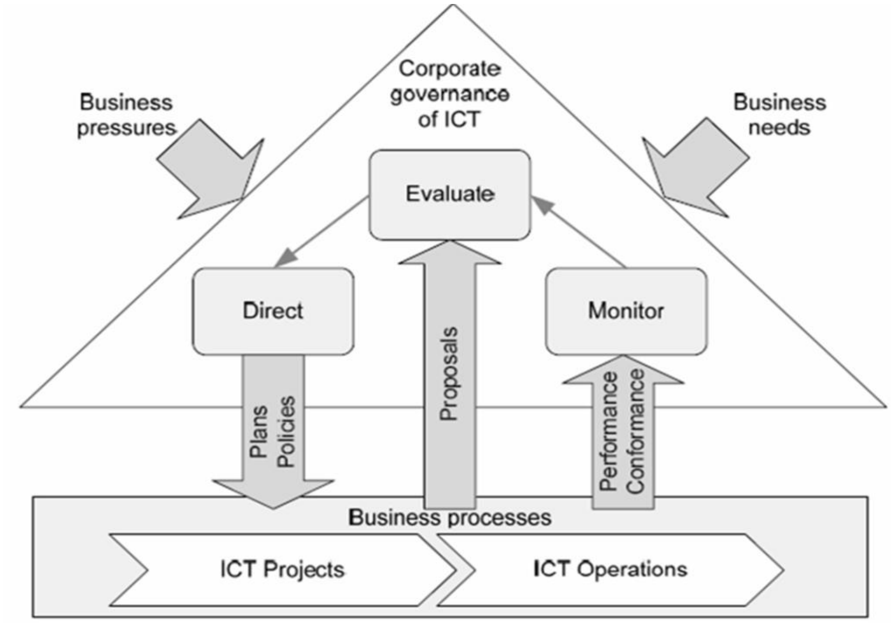


Figure 15: Model for corporate governance of IT (ISO, 2008).

III. IT Governance for SME

The previous chapters provided a solid overview about IT governance and the relating frameworks. This chapter narrows the scope down to IT governance for small and medium-sized enterprises. The priory envisaged frameworks and standards are addressing more large companies because of the effort that has to be taken for proper implementation and establishment of such a framework. This chapter first enlists the obstacles for small and medium-sized enterprises that interfere the existence of governance structures and activities based on former research in this area of interest. In a second step, prior research activities in this particular area of interest are investigated.

Both, the identified obstacles and the look at existing literature is a vital step for the development of the framework. The obstacles draw attention to possible challenges and the results of the carried out research activities provide valuable input for the structural design of the framework.

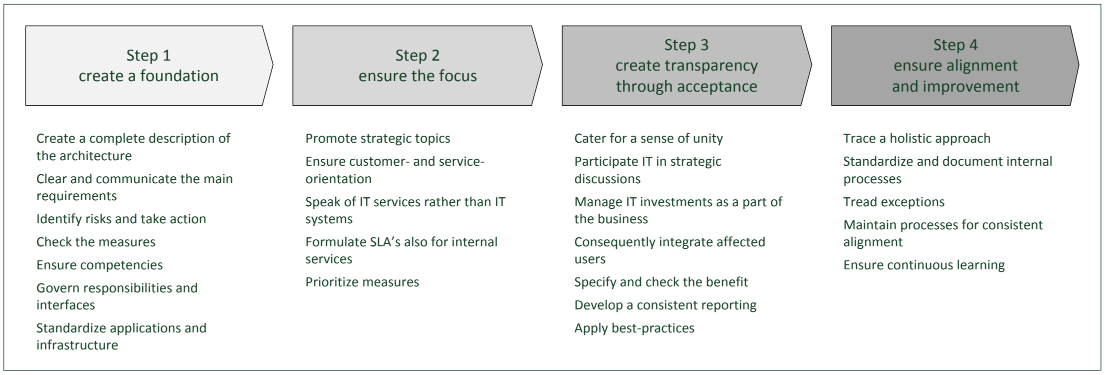
1. Obstacles

Bitterli (2011) claims in his article “IT Governance – auch für KMU notwendig und sinnvoll” that small and medium-sized enterprises focus their IT related efforts to encounter the challenges that emerge during the daily business. Therefore, small and medium-sized enterprises often lack of a clear strategic planning in IT because they just do not have enough resources for that. This results in the fact that although the daily IT business is under control, small and medium-sized enterprises are facing serious troubles when they for example want to introduce a new application or migrate an application to a newer platform. This leads to the apprehension that, if small and medium-sized enterprises are not even able to manage predictable changes, it becomes even more chaotic and uncoordinated when something unpredictable happens. This could be for example an internet attack or malfunctioning hardware.

Information becomes a key factor of production. This of course also holds true for small and medium-sized enterprises and the way to handle information may be the source of a competitive advantage. Unlike any other factor of production, information has requirements regarding their availability, integrity or reliability, just to mention some of them. The demand against information processing is growing and the main problem is that small and medium-sized enterprises are not able to respond this demand in an appropriate manner. Customer data for example has to be accessible all the time and from everywhere over the internet. It is not difficult to develop a customer relationship management (CRM) system which is accessible over the internet that covers this demand but the crux of the matter is that this business requirement, the accessibility of customer data, has to be ensured. If we continue with this example ensuring this specific business requirement means that the accessibility of the CRM system has to be guaranteed. To be honest, it is no witchcraft to set up CRM system and making it accessible from the internet but has be proven very hard to ensure that the CRM system is up and running within the defined service time. There may be a plenty of subsystems that the CRM system relies on, patches and updates have to be installed, backups have to be scheduled and the network and the whole IT infrastructure have to be maintained and secured against unauthorized access. And so it comes that an easy business requirement implies a number of IT specific activities that have to be executed however they do not have direct impact to the business requirement itself. This casual chain requires proper management and therefore, good IT governance is a key part when managing information (considered here as the factor of production). And this is the most challenging part in IT and also the place where small and medium-sized enterprises often feel overwhelmed. Another obstacle in the implementation for IT governance in small and medium-sized enterprises is that the existing frameworks are oversized and little companies just cannot afford IT governance.

2. Previous Research

Various research activities have examined whether proper IT governance activities have a positive effect to the business success. In his paper, Landolt (Lohnt sich IT-Governance auch für KMU - Eine empirische Untersuchung schweizerischer Industrieunternehmen, 2009) states that the need for governance-alike structures increases with the size of a company and there is a clear correlation between the maturity of the companies IT governance and the size of staff. On the other hand Landolt’s research could whether prove nor discard the necessity of good IT governance to improve IT related decision making. The main statement of his research is that sensible embodiment of IT governance is highly individual because of the interaction of several relevant factors. But he clearly states that the placement of a good foundation for effective governance and control of IT is essential for business success. Landolt has therefore developed some generic guidance that supports small and medium-sized enterprises with the implementation of IT governance. The following figure briefly introduces the guidance developed by Landolt.



Step 1
create a foundation

- Create a complete description of the architecture
- Clear and communicate the main requirements
- Identify risks and take action
- Check the measures
- Ensure competencies
- Govern responsibilities and interfaces
- Standardize applications and infrastructure

Step 2
ensure the focus

- Promote strategic topics
- Ensure customer- and service-orientation
- Speak of IT services rather than IT systems
- Formulate SLA’s also for internal services
- Prioritize measures

Step 3
create transparency
through acceptance

- Cater for a sense of unity
- Participate IT in strategic discussions
- Manage IT investments as a part of the business
- Consequently integrate affected users
- Specify and check the benefit
- Develop a consistent reporting
- Apply best-practices

Step 4
ensure alignment
and improvement

- Trace a holistic approach
- Standardize and document internal processes
- Tread exceptions
- Maintain processes for consistent alignment
- Ensure continuous learning

Figure 16: Growth trajectory of IT governance, following (Landolt, 2009, p. 91).

In step 1, the basis for successful governance activities is laid. The description of the IT-architecture, the gathering of the requirements and initial risk management practices can be considered to be the starting point for the IT governance initiative. Once this is done, competencies, roles and responsibilities can be determined. This step is concluded by harmonizing the IT environment. Step 2 extends the scope with strategic thinking and introduces service-management mindset within the company. The primary goal is to create measurable IT services to be able to assess their contribution to the business, which is a foundation for the next step. Step 3 promotes the strategic alignment of the IT. This is done by involving IT in business decisions such as strategy workshops and investments. Also transparency can be improved through reporting (based on SLA). In step 4, IT processes become integrated in the whole company process landscape.

The research paper of Kopp (2009) goes into the same direction. Although he also does not provide an IT governance framework for small and medium-sized enterprises, he proposes a six step implementation approach. First, a common understanding has to be created and IT processes have to be analyzed and assessed regarding their importance. In a next step, he proposes to map the existing processes to the processes described in the various frameworks. This activity could be seen as some kind of tailoring and is an interesting approach to align the existing IT processes to the ones described in the respective framework. Then the proposed actions are implemented and evaluated.

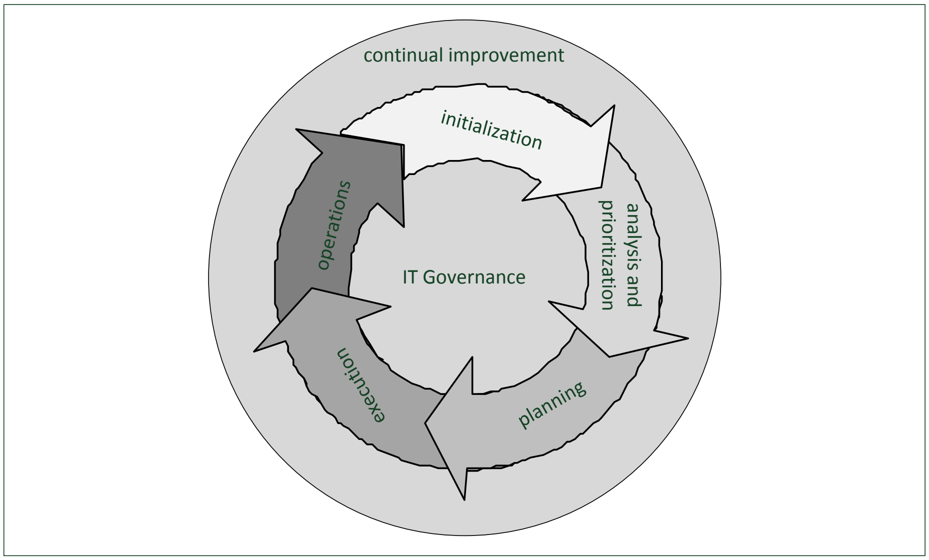


Figure 17: Phases for IT governance implementation (Kopp, 2009, p. 74).

This implementation approach provides a methodology for implementing IT governance structures in small and medium-sized enterprises, based on the importance of the existing IT processes. But there is still much effort that has to be put in and the author believes that for smaller companies, the expenditures for such a project are still too high.

Kunz (2011) takes another approach for IT governance for small and medium-sized enterprises. He subdivides small and medium-sized enterprises into five different types. The basic idea is that a company that wants to implement governance functions for their IT has first to find out to which type she belongs to. The types are distinguished regarding their size and the IT significance. The findings of his research are that IT governance for small and medium-sized enterprises cannot be generalized allowing the adoption of the proposed types. Because of the vast distribution of requirements he proposes that it would be rather more efficient to define an own IT governance framework for each company, however the proposed governance activities within the type could be taken as a starting point.

Another study published in the ISACA Journal (Busta, Portz, Strong, & Lewis, 2006) identified the key IT controls of small and medium-sized enterprises. To find out these controls, an expert group was invited and was given the opportunity to select the most important IT controls out of 30 available controls that are available in COBIT 3. The survey was conducted based on the delphi method. The result of the study is (see Figure 18) that security and backup activities are ranked on top of the most important it controls, followed by planning activities such as IT strategy and continuity planning.

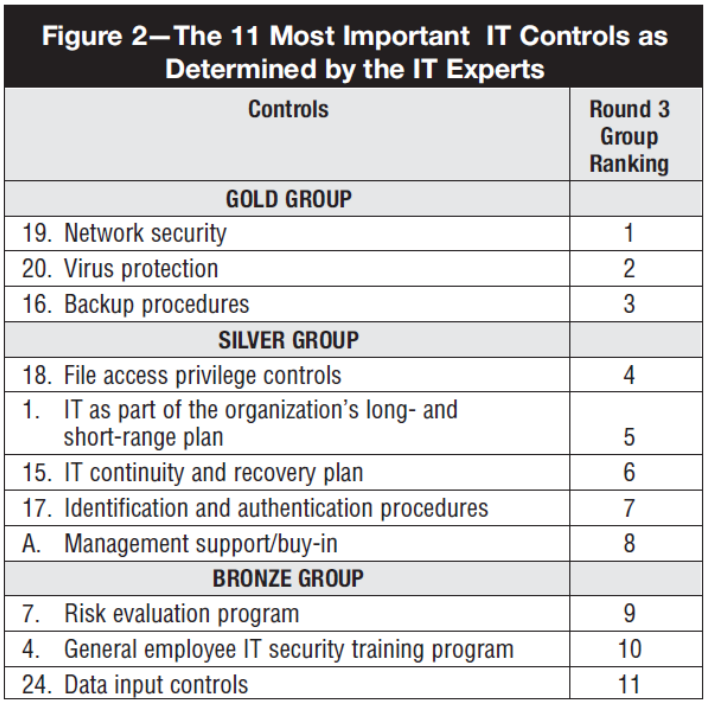


Figure 2—The 11 Most Important IT Controls as Determined by the IT Experts

Controls	Round 3 Group Ranking
GOLD GROUP	
19. Network security	1
20. Virus protection	2
16. Backup procedures	3
SILVER GROUP	
18. File access privilege controls	4
1. IT as part of the organization's long- and short-range plan	5
15. IT continuity and recovery plan	6
17. Identification and authentication procedures	7
A. Management support/buy-in	8
BRONZE GROUP	
7. Risk evaluation program	9
4. General employee IT security training program	10
24. Data input controls	11

Figure 18: Top IT controls (Busta, Portz, Strong, & Lewis, 2006, p. 2).

The survey states that by implementing these IT controls, a small business can greatly improve the security, reliability, strategic use and accuracy of its IT resources. But also here, the key question of how to implement such governance mechanisms is not answered

2.1 Upshot

The obstacles that small and medium-sized enterprises face when implementing IT governance can be attributed in a large part to the brevity of IT resources. Small and medium-sized enterprises seem unable to put more effort into proper governance of enterprise IT, be it due to financial limitations or insufficient prioritization. On the other hand it can be stated that the requirements regarding stable and efficient IT processes are not much lower than the requirements that are posed against IT in large companies. In order to be able to find out these specific requirements, it is necessary to conduct some further research. The research design and the findings will be presented in chapter IV.

The above introduced research papers all have in common that IT governance helps a company in managing their IT processes. They also reveal that the existing IT governance frameworks cannot be adopted in small and medium-sized enterprises because of their scope and the effort that has to be put for implementation. None of the above mentioned research papers provide simple guidance for implementing IT governance based on the company’s requirements, regardless of being compliant with the existing frameworks. To conclude, the challenge in this situation is to design a suitable framework tailored to the needs of small and medium-sized enterprises by taking into account that the companies are not able to put much additional effort into the implementation and maintenance of such a framework.

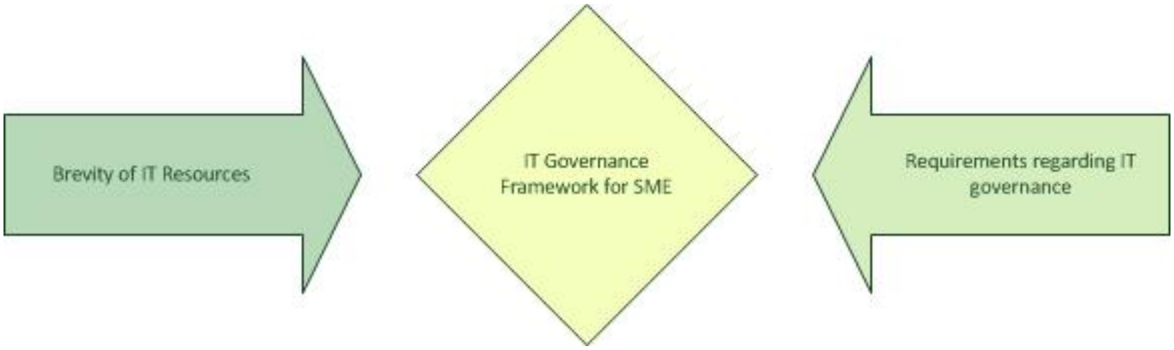

Brevity of IT Resources
IT Governance Framework for SME
Requirements regarding IT governance

Figure 19: Challenge for the framework design.

In the broadest sense, this circumstance could be described as a constraint-satisfaction-problem. The resource problem and the requirements for the IT governance framework depict the constraints that set the range of possible solution. The challenge is to find a suitable framework, above illustrated with the yellow rhombus that fulfills both constraints. However finding an appropriate framework for IT governance for small and medium-sized enterprises is not a computable problem because both constraints are not quantifiable. Nevertheless the consideration of the constraints is vital to find a good solution.

IV. Research

This chapter explains the research methodology that has been chosen to develop the IT governance framework for small and medium-sized enterprises.

The findings of the previous chapter require further investigation of the requirements that are posed against an IT governance framework for small and medium-sized enterprises. Therefore, a research activity was launched to identify the key requirements.

1. Research Design

In this chapter, the research activity is introduced with regard to the underlying hypothesis and the scope of the research activity. It also provides an overview about the overall research proceeding. Finally, the research activity is classified according to the research onion (Saunders, Lewis, & Thornhill, 2004).

1.1 Hypothesis

This papers underlying hypothesis is that the existing IT governance frameworks presented in the prefacing chapter are not applicable for small and medium-sized enterprises and that there is a more effective way of how IT governance can be addressed within small and medium-sized enterprises. In more detail, the hypothesis can be formulated as follows:

"IT governance in small and medium-sized enterprises leaks of proven implementation guidance and a suitable common agreed framework. A combination and tailoring of existing frameworks, which are mainly applicable for large organizations (including CobIT, ValIT, RiskIT, ISO27000, CMMI), will be a possible solution to provide a baseline IT governance approach for small and medium-sized enterprises."

Important to notice is that the hypothesis does not argue that the already existing frameworks cannot be applied within small and medium-sized enterprises. But it states that there are more effective ways of how IT governance principles can be implemented within smaller companies. This is expressed by the sentence that by tailoring and combining these big frameworks into a smaller framework, IT governance can be implemented much easier. Of course all the big frameworks can also be implemented and have equal validity towards the framework that is being developed in this paper. However, the implementation of these frameworks requires on the one hand significant personal and organizational resources and, on the other, is in a large part too extensive with regards to the scope and the level of detail.

To conclude, the statement suggests that existing standards, principles and methodologies for managing IT governance should be adapted to the dedicated needs of smaller and medium-sized enterprises.

1.2 Scope

The framework should be appropriate for the usage within small and medium-sized enterprises. Therefore it is vital to have a precise description of what small and medium-sized does mean in this context. Although there is no common agreed definition of small and medium-sized enterprises available, a quantitative distinction can be made according to the definition of the European Commission (Europäische Kommission, 2006) where small and medium-sized enterprises are categorized related to their size of staff, the turnover and the balance sheet total.

	Staff size	Turnover (M./Euro)	Balance sheet total (M./Euro)
Minimal enterprises	< 10	≥ 2	≥ 2
Small enterprises	< 50	≤ 10	≤ 10
Medium enterprises	< 250	≤ 50	≤ 43
Large enterprises	≥ 250	> 50	> 43

Table 2: European definition of company sizes (Europäische Kommission, 2006).

A qualitative distinction between large enterprises and small and medium-sized enterprises can be made by emphasizing the differences in the company management. In his book, Pfohl (Unternehmensführung. In Betriebswirtschaftslehre der Mittel- und Kleinbetriebe.Grössenspezifische Probleme und Möglichkeiten zu ihrer Lösung, 2006) enlists typical differences in operational management and organization.

SME	Large enterprise
Company owner – entrepreneur	Manager
Paternalistic management	Management-by principles
Big significance of improvisation and intuition	Slight significance of improvisation and intuition
Little planning	Extensive planning
Person-oriented labor division	Task-oriented labor division
Close to the business	Distant for the business
Direct communication line	Prescribed communication line
Instruction and control in direct personal touch	Formalized and impersonal instruction and control relationship.

Table 3: Differences betw. SME and large companies in management style (Pfohl, 2006, p. 18f).

These differences should be taken into account for the framework design. Another important indicator identified by Hamer (Betriebswirtschaftslehre der Mittel- und Kleinbetriebe. Größenspezifische Probleme und Möglichkeiten zu ihrer Lösung, 2006, pp. 25 - 50) for a distinction between large or small and medium-sized enterprises is whether the company owner still takes managerial functions or he concentrates on strategic functions. Hamer calls this differentiation the threshold of growth. At this point where entrepreneurs are no longer involved in the daily business a company approaches the qualitative definition of a large enterprise. Fast growing enterprises often face the challenge to find the balance in their organizational structure (agile versus formalized structure).

The above expounded quantitative and qualitative distinction approaches are a good possibility to set the scope for this IT governance framework. However, a precise setting of the scope is due to the still remaining uniqueness of each company not possible (Leitner, 2001, p. 53). The industry sector or country specific factors are variables that make it impossible to find a universal definition for small and medium-sized enterprises. Nevertheless, a certain categorization has to be done in order to be able to audit the hypothesis. The IT governance framework for small and medium-sized enterprises adheres to the definition of the European Commission and puts the focus to small and medium enterprises, meaning that the framework fit best to the demands of enterprises that have about 50 to 250 employees with an annual turnover of between 10 and 50 million and a balance sheet total from 10 to 43 million. In the best case, these companies also exhibit qualitative characteristics of small and medium-sized enterprises.

To summarize and concentrate the scope, the IT Governance Framework developed in this paper is best suitable for:

- Enterprises with 50 – 250 employees
- Enterprises that are managed with strong characteristics appropriate for SME’s

1.3 Research Procedure

In order to be able to prove the hypothesis, the following procedure has been selected. The following subchapters briefly explain the procedure.

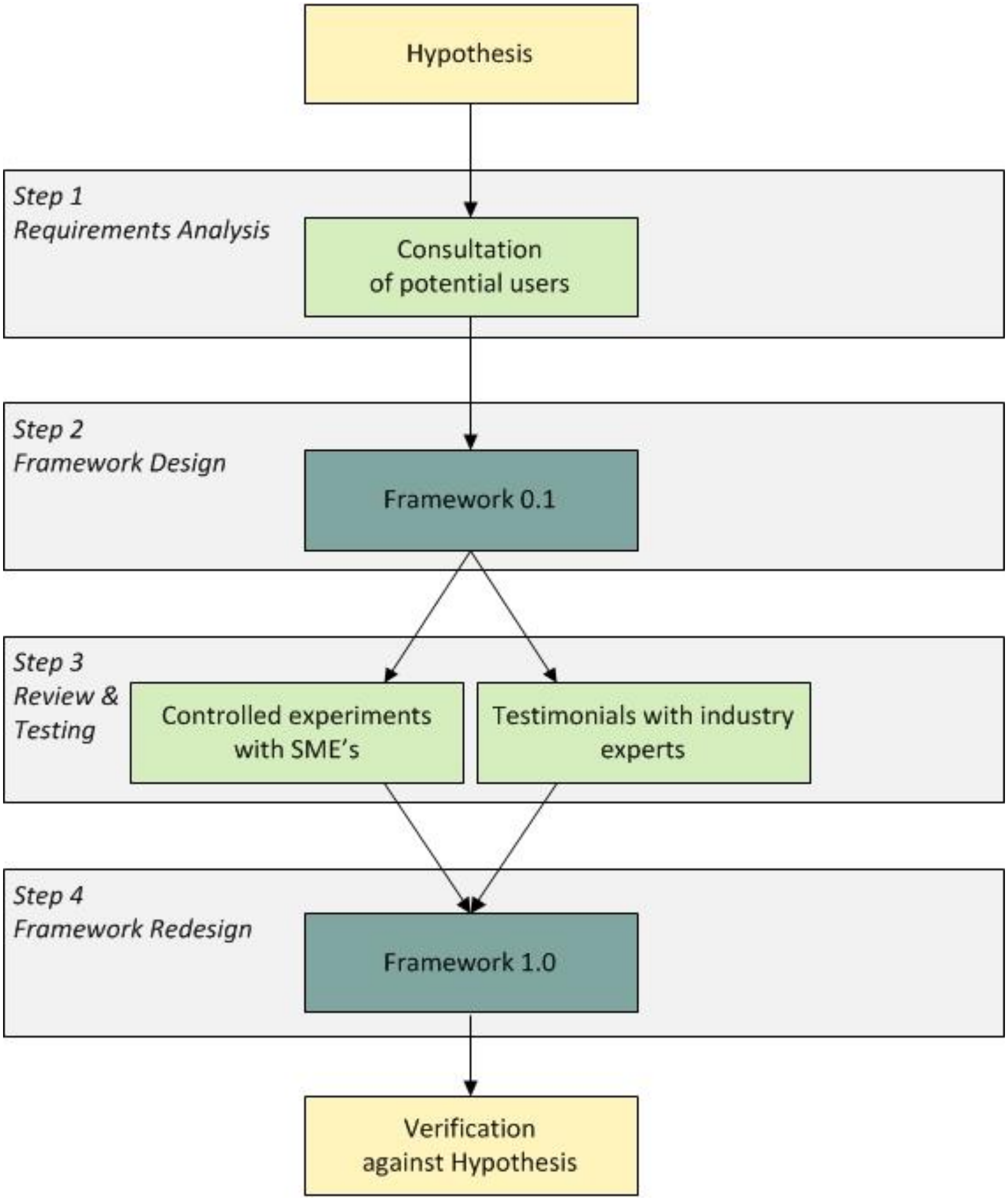


Figure 20: Research procedure.

1.3.1 Step 1 - Requirements Analysis

The requirements analysis is the first step for the development of the IT governance framework for small and medium-sized enterprises. Its main goal is to identify the key needs of small and medium-sized enterprises regarding IT governance. In this research, greatest importance has been attached to this phase of the research cycle. On the one hand, not much field research in this area of interest has been conducted so far and therefore it is not possible to rely on existing research findings. On the other hand, the steadily changing conditions in the IT sector make it hard to find some generally applicable statements in terms of IT governance for small and medium-sized enterprises. Because of this situation, an own field research activity has been initiated. The output of the requirements analysis serves as the starting position for the framework design.

1.3.2 Step 2 - Framework Design

The framework design should adhere to the findings in the requirements analysis, by trying to cover most of the requirements and putting them together in a single and consistent framework. In this paper, an initial draft of the IT governance framework for small and medium-sized enterprises is designed. This draft (Framework 0.1) is used as input for the review and testing step.

1.3.3 Step 3 - Review & Testing

Review and testing is a vital part in the development cycle. The purpose of the review activity is to assess the framework from a theoretical perspective by industry experts. In this step, conceptual discrepancies and other potential comprehension issues are addressed. As a positive side effect, testimonials written by industry experts help to improve the credibility and validity of the framework. With testing activities, the degree of fulfillment regarding the requirements analysis can be made. This enables to make qualitative assertions whether the set requirements are covered by applying the framework in practice. By doing some testing, practical experience can be gained and it also offers a good possibility to revise the framework. To summarize, the goal of the testing activities is to prove whether the requirements have been fulfilled and to reveal the weak spots of the framework. With these review and testing activities, it should be possible to make a precise statement whether the hypothesis is true or wrong.

1.3.4 Step 4 - Framework Redesign

In the step of the framework redesign, all findings from the review and testing phase are consolidated and implemented in the final version of the framework. It is important to notice that this step is not essential to test the hypothesis but considering that the IT governance framework for small and medium-sized enterprises can be considered as some kind of a product, it it's therefore meaningful to include this last step into this master thesis in order to have a complete and consistent result.

1.4 Classification

To classify this research activity, the research onion (Saunders, Lewis, & Thornhill, 2004, p. 528) from Saunders can be used. The research method is explained by starting at the center of the onion.

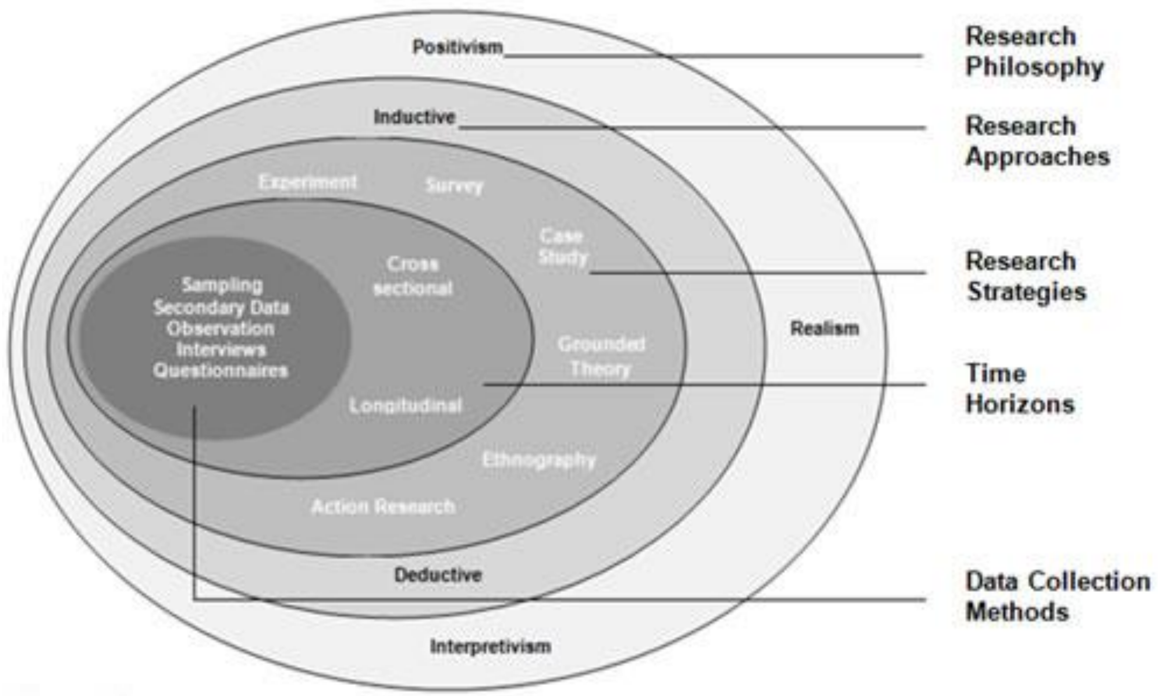


Figure 21: The research onion.

The data collection is a combination of secondary data, questionnaire and interviews. The analysis of the already existing frameworks and research papers in this area of interest is made to obtain a basic understanding of the topic and to get an overview about the current research activities. The study of the existing frameworks also provides valuable input for the research as well as the framework design. The questionnaires haven been designed to find out the needs of small and medium-sized enterprises regarding it governance and to be able to recognize the challenges they face. Within the questionnaire, the participants are asked to rate the perceived importance and the importance of the respective IT topic. These insights provide valuable quantitative input for the fundamental design of the framework. The conducted interviews with small and medium-sized enterprises bring qualitative input for the design of the framework. One may argue that conducting interviews with only two participants is not enough to have a representative population but the author believes that the basic requirements regarding IT governance are quite similar across all small and medium-sized enterprises. In a further step, an initial draft of the framework was sent to a peer-review and a little field test in one enterprise. The experts were asked to judge the framework regarding the structure and the content whereas the enterprise put the focus on the applicability of the framework. This cross-validation is an essential step to prove the hypothesis. The expert opinion is made for obtaining a statement concerning the validity of the framework from a scientific point of view. The field test is made to obtain a statement of applicability. The main proposition of the statement of applicability should testify that IT governance can be implemented faster and in a more efficient way by using the framework developed in this paper. By conducting these two activities, once from a scientific and once from a practical perspective, the validity and the applicability of the framework is tested by all relevant stakeholders.

The time horizon is cross sectional and the chosen research strategy has the form of a survey. The research approach is rather deductive, since already numerous it governance frameworks for large companies exist and there has been some research in this the specific subset of it governance for small and medium-sized enterprises. This research has shown that proper it governance has positive impact for the business value. The research methodology belongs to the positivism research philosophy.

2. Research Findings

This chapter summarizes the research findings of the requirements analysis and the review and testing phase. The main objective of the requirements analysis is to create a basis of decision making for the framework design. The goal of the review and testing phase is then to refine the content of the framework, which is done by peer-reviews, and to have a statement of applicability from a small and medium-sized enterprise.

2.1 Requirements Analysis

The requirements analysis is divided into two parts, a survey and interviews. For the accomplishment of the survey, seven small and medium-sized enterprises were identified and surveyed. Due to privacy reasons, all participants wished that the questionnaires were anonymized. The goal of the survey is to provide a quantitative basis of decision making for the framework design. Furthermore, a structured interview was conducted with two of the above mentioned participants. The goal of the interviews is to provide specific qualitative input for the content of the framework.

2.1.1 Survey

The survey addresses all IT relevant activities and the participants have to assign for each activity their respective maturity level and estimate the overall importance the activity has. The assessment of the maturity can be easily done by selecting the most appropriate description of the activity that is predefined in the questionnaire. The importance is estimated in relative terms (very important, important, rather important and unimportant). All questionnaires can be found in the appendix.

This methodology is based on the process model developed by the “Fachstab für Informatik der Treuhand-Kammer” of Switzerland and it was published in 2010 (Fachstab für Informatik der Treuhand Kammer, 2010). Its original purpose is to provide guidance for an internal IT risk assessment and the author believes that putting the risks in front is the right approach to deal with IT governance. The original process model consists of 20 subject areas and 88 questions. A little tailoring to reduce the scope has been made by the author, resulting in 18 subject areas and 66 questions.

The following figure depicts the consolidated results of all participants.

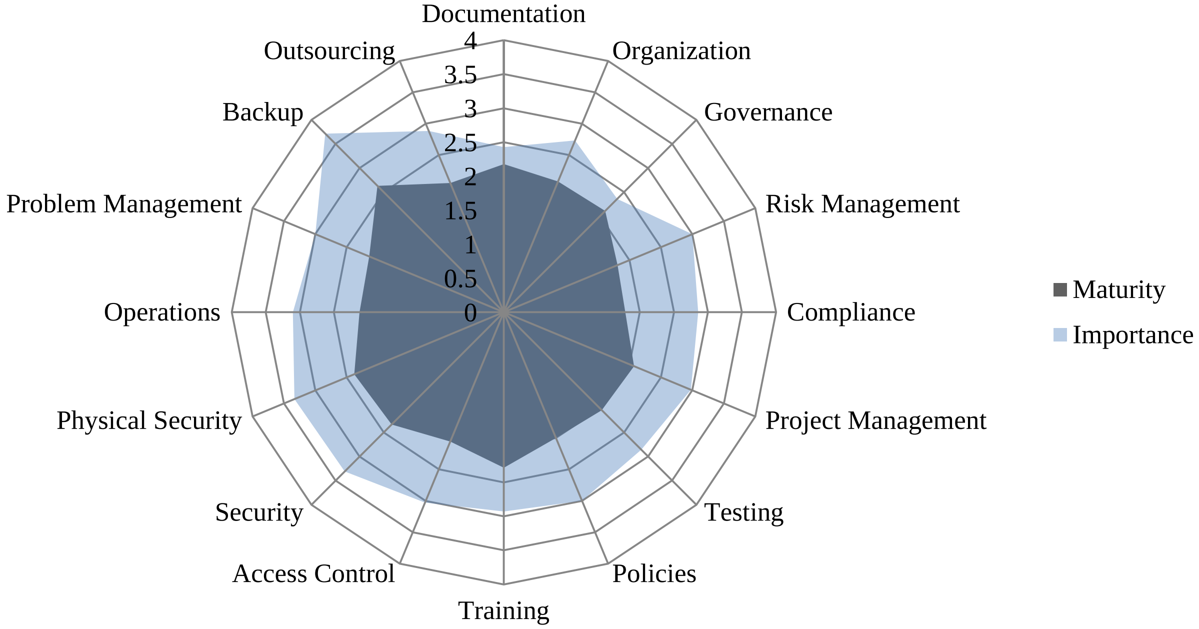
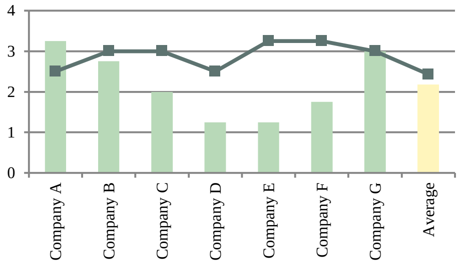
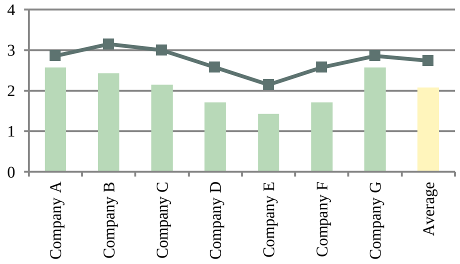
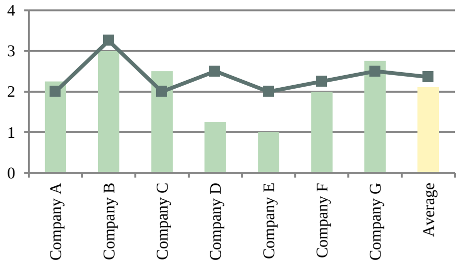


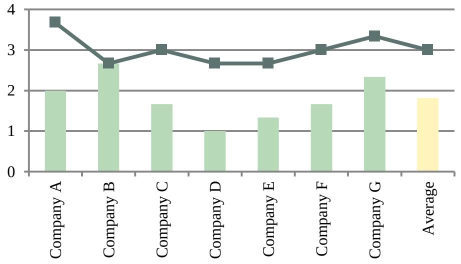
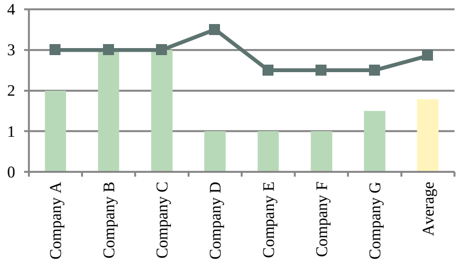
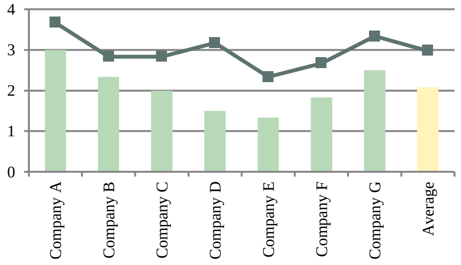
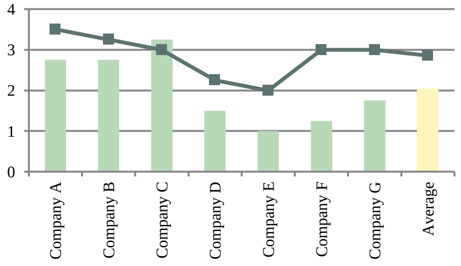
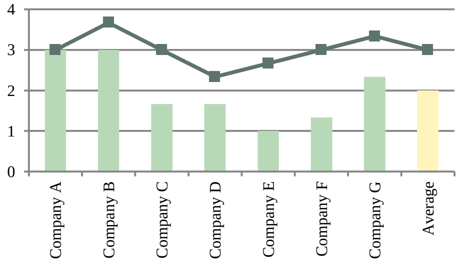
Figure 22: Consolidated results of survey.

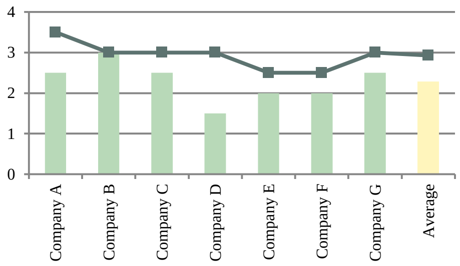
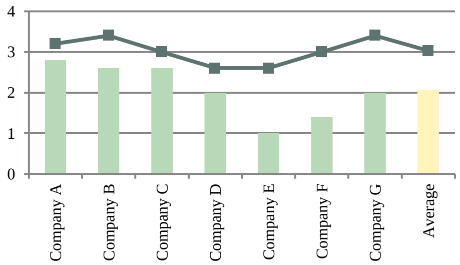
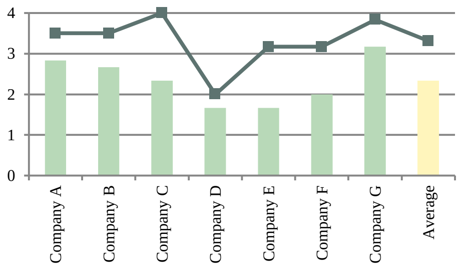
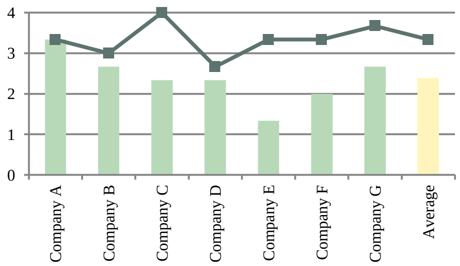
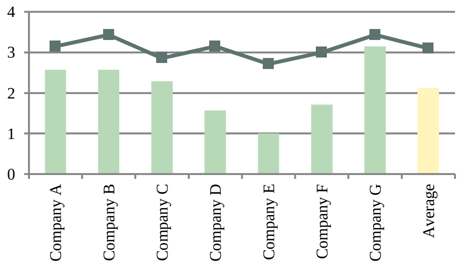
At a first glance it is easy to recognize that, for every activity, the rated importance is higher than the stated maturity. It would be misleading to conclude that a direct comparison between maturity and importance can be made. This is not reasonable because on the one hand, the displayed results are average values and on the other hand, the two comparative values do not stand in direct correlation to each other. For example, the average importance stated by the survey participants for backup was rated 3.7, which means that proper backup and recovery routines are considered to be very important. The stated maturity was rated 2.6 and a maturity level between two and three already implies that regular backup is scheduled and controlled. This example should express that a lower maturity level, compared to the importance, does not testify that the activity is badly executed. Regardless of this fact, a general assumption can be made saying that the surveyed small and medium-sized enterprises still have potential for improvement concerning their process maturity.

The figure also reveals that the surveyed enterprises have a quite balanced maturity level across all their internal IT processes and there are no outliers. When the enterprises maturity levels in the different activities are considered isolated, there is only one company where this statement does not apply (see Appendix A – Consolidated Survey Results).

This coherent balance predicates that the examined small and medium-sized enterprises consider all relevant IT processes. The following table provides a detailed analysis for each activity. In each chart, the bars indicate the maturity level and the line illustrates the importance. All values must have been between one and four.

	Average Values	Comment
Documentation		Documentation contains all IT relevant documentation activities such as hard- and software inventories, specifications and an overview about the system landscape. Relevant criteria in this activity are the topicality of the respective documents. Whereas the importance is quite stable at the participants, the maturity varies from low to high. Documentation is considered to be a painstaking task and the value contribution is very hard to measure. The value of good and actual documentation appears when the IT infrastructure has to be changed or updated.
Organization		In this activity, topics like responsibility, segregation of duty and substitution within the IT department are addressed. All participants stated that the responsibilities and substitution within IT are clear, however not explicitly documented. The segregation of duties proves hard to implement. The limited company size and the missing role-based division of tasks may be an explanation for the lower maturity level. The question whether the company belongs to the early-adopters or the followers when it turns to procurement is also part of this activity and all of the participants denoted themselves to be followers, which means that new technologies are not instantly applied but rather solid and proved components are applied. This circumstance may be argued with the fact that small and medium-sized enterprises want to rely on stable technology in order to prevent from possible early-adopter drawbacks and rather take the risk of a possible loss of productivity.
Governance		Governance encompasses IT-business-alignment, service level agreements and business process management. For this activity, the overall rated importance is the lowest amongst all examined activities. None of the companies has written service level agreements nor official processes that improve IT-business-alignment. However, there are formal processes that cover the management of IT processes. Small and medium-sized enterprises typically follow a rather short-terminated decision-making basis which is a possible explanation why the importance was considered to be lower. On the other hand, fast decision-making enables great agility which is a core advantage of any small and medium-sized enterprise towards large companies.

	Average Values	Comment
Risk Management		Risk management is obviously considered to be very important but in contrast, the stated maturity level is one of the lowest across all examined activities. Most companies do not have formal risk management procedures in place and appropriate security measures are only taken after safety-relevant incidents. A possible explanation for this imbalance is that the strong focus to the daily business prevents from the implementation of proactive risk management procedures.
Compliance		Compliance deals with conformity with respect to laws and regulations. The importance was rated high and the maturity level varies from low to high. A reason for this big difference is that compliance requirements are strongly depending on the respective industry sector. Companies B and C both are in the industrial sector where rigorous restrictions are in place. The other companies are in the services industry where the requirements concerning the compliance to external laws and regulations are not as obvious as in the industry sector, meaning that companies are not fully aware of the existence of such additional requirements.
Project Management		All companies have some project management processes in place and have an accurate overview about the running projects. However, projects leak of formal project leaders and the assignment of a project team. This leads to the situation that responsibilities are not clearly assigned and the commitment to the project is lower than it could be with the existence of official project teams. The company size of most participating companies and hence the proximity of the IT staff allows this loos project management approach.
Testing		Testing not only involves proper testing of new applications or changings in the infrastructure but also regards the physical segregation between testing and productivity environments. Companies in the industrial sector tent to put larger emphasis on solid testing mechanisms in isolated environments whereas the service industry often conducts testing activities in the productive environment. Also the rated importance follows this pattern at large.
Policies		The existence of and adherence to policies is considered to be important. In most companies, policies regarding the use of e-mail, internet or external data devices (for example USB sticks) are in place but are not actively traced towards the adherence. Also policies concerning data-archiving was examined in under this activity where companies showed a rather low maturity level. Data-archiving requires special software and additional infrastructure and is therefore treated like deluxe topic within the surveyed companies.

	Average Values	Comment
Training		Training deals with specific end-user training on specific applications and general IT training. For most small and medium-sized enterprises, learning by doing is the preferred education measure, for specific application training as well as general IT training. The surveyed companies also stated that the documentation material for specific applications is in most cases not complete and outdated. However, general IT training is rated at a higher maturity level than specific application training. In small and medium-sized enterprises it is mostly not economic to develop own training material and this is a reason why specific IT training is rated slower than general IT training that can be obtained out-of-the-box.
Access Control		Impersonal user accounts, authentication mechanisms and appropriate password policies are addressed in the activity access control. The size of the company seems to play a crucial factor that has direct impact to these issues. In small companies, the division of labor is typically low and one employee takes several roles and responsibilities. A proper rights and access management would hinder the productivity and means that much has to be taken to realize such a system which is not reasonable for very small enterprises. However, access control is considered to be a top priority issue regarding the rated importance.
Security		Security covers various security measures such as virus control and network protection as well as administrative privileges at the workstations and remote access (VPN). Excluding company D, security was rated to be one of the most important activities within the IT department. Virus control and network security is already executed at a very high maturity level whereas remote access and administrative privileges are not yet implemented in a mature way. The reason for this may be that the configuration of remote access requires expert knowledge. The problem with administrative rights is omnipresent in small and medium-sized enterprises.
Physical Security		Access to the sites, fire prevention and interruption-free power supply were assessed under physical security. The varying maturity value among the surveyed companies can be explained with the argument of the company size. Very small enterprises often only have one single site and also only one server infrastructure. Much effort would arise in order to properly secure this infrastructure and economies of scope and scale would not apply. However, the physical infrastructure has to be secured which is confirmed through the rated importance.
Operations		Operations summarize activities like configuration management, monitoring and control and operational task sharing. Small and medium-sized enterprises often cannot engage dedicated IT administrators but rather assign the responsibility to the IT staff. In some cases even non-IT employees have to take care about easy IT operational tasks where external experts are consulted for complex changings in the infrastructure.

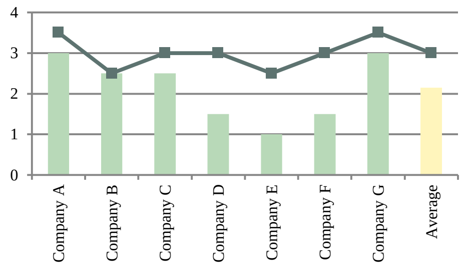
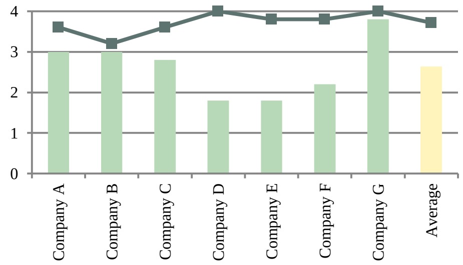
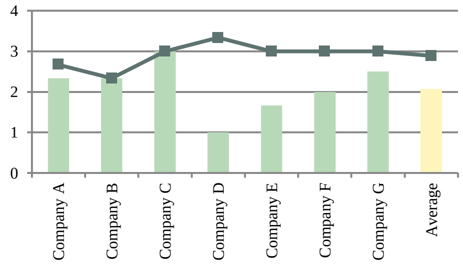
	Average Values	Comment
Problem Management		Dealing with problems, incidents and support requests is summarized under the term problem management. The small companies among the surveyed participants do not have a central contact point for incidents and support requests in place. Problems and incidents are treated ad-hoc directly with the involved departments. The larger companies all have established some kind of a help-desk, although still not professionally managed. The operation of a call center is not profitable for a small and medium-sized enterprise.
Backup		Backup was rated the most important amongst the surveyed activities. A serious backup process not only covers the regular execution of backups of data, applications and systems, also recovery testing is an inevitable part in the backup and recovery processes. All companies stated that they have regular backup processes in place and also store their backup on more than one location. Recovery tests are not scheduled at every company such as the existence of an IT emergency plan. The emergency plan contains instructions on how to behave in case of emergency, which applications are considered to be the most important ones to protect and recover as quick as possible.
Outsourcing		Business partners are an elementary part in the production chain of every enterprise. The dependence on external partners is highly conditional to the respective industry, which is an explanation for the heavily varying statements regarding the maturity in dealing with external partners and suppliers. Despite the fact that any of the surveyed companies indicated that outsourcing contracts are centrally managed, the agreements are not traced with regard to their level of fulfillment.

Table 4: Survey results analysis.

The survey results analysis is the basis for the fundamental design of the framework. Backup, security and stable operations are rated the most important, followed by problem and project management. Testing, organization, documentation and governance are rated to be less important.

Topic	Average
Backup	3.71
Physical Security	3.33
Security	3.31
Operations	3.10
Access Control	3.03
Risk Management	3.00
Policies	3.00
Problem Management	3.00
Project Management	2.98
Training	2.93
Outsourcing	2.89
Compliance	2.86
Testing	2.86
Organization	2.73
Documentation	2.43
Governance	2.36

Table 5: Survey results - average importance.

These results allow the conclusion that all operative processes that have a strong impact to the daily business are rated with a high importance. Solid backup mechanisms, a clear security baseline and stable operations of the applications are the core requirements for any business regarding information technology. Another impact factor may be that small and medium-sized enterprises have to prioritize their IT activities because the small budget and the limited resources. This argumentation also explains why rather organizational tasks like documentation and governance are considered to be less important.

A similar result was reached when considering the perceived maturity level of the respective process. Similar to the statements regarding the importance, backup and security remain the forerunners.

Topic	Average
Backup	2.63
Physical Security	2.38
Security	2.33
Training	2.29
Documentation	2.18
Problem Management	2.14
Operations	2.12
Governance	2.11
Organization	2.08
Project Management	2.07
Access Control	2.06
Outsourcing	2.06
Testing	2.04
Policies	2.00
Risk Management	1.81
Compliance	1.79

Table 6: Survey results – average maturity.

To summarize, the survey provided valuable information. It has to be taken into account that the measures illustrated in the previous tables are average values and therefore have to be considered with a certain restraint. Nevertheless the results can be used for the framework design. According to the survey results, the framework should primarily focus on operational topics like backup, security and operations.

Another insight that the survey provides is that every enterprise is different regarding the importance of their IT processes, may it be because of their industry sector or regional impacts. Therefore it would be best for the enterprises when they are supported with some kind of guidance for the implementation of an IT governance framework. This insight has crucial impact to the prescribed implementation process which is included in the framework.

2.1.2 Interviews

In the interview, the same IT governance topics as in the survey were addressed and the participants were asked to describe their internal procedures concerning these topics. Additionally, the interview addressed questions regarding the daily challenges that IT departments face and the future requirements that are posed against them. In the following, a short extract of each interview with the consolidated findings is presented.

Findings of the Interview with Martin Zurbrügg, Informaticon AG

Informaticon AG counts 40 employees and its core business is the development and distribution of their own enterprise resource planning (ERP) solution. They also have a small department that sells hard- and software to their customers to provide one-stop solutions. The IT department consists of three employees and is led by Martin Zurbrügg.

In the following, a short extract of the interview is provided:

> *"A huge advantage of small and medium-sized enterprises is that the decision making process is usually much faster and more flexible than in large companies"* (Zurbrügg, 2012)

The organization of smaller companies is often not that structured than it is in larger companies. Decisions do not have to pass through a formal process but can be discussed with all involved.

> *"Changes in the infrastructure are usually done without proper testing in advance. With the limited resources, it is hard to set up serious testing scenarios. This sometimes leads to unsolicited outages." (Zurbrügg, 2012)*

In software development, testing is a vital task in the deployment procedure. The testing of software components can be realized with little effort whereas the testing of the productive setup is difficult to manage. How can it be assured that the release of the software will work on the underlying infrastructure? Is the data still available and does not become changed through the installation procedure of the release? These questions can only be replied if staging levels are applied and this is rarely the case in small and medium sized enterprises.

Top-three challenges in the future:

- Scalability and performance requirements
- Cross-linkage of sites
- Mobile office

The scalability and performance requirements are mainly addressed to infrastructure components as network and computing resources. Zurbrügg says that it is hard make an estimation of the future needs because of the always changing and growing requirements. Performance usually cannot be seriously measured in small and medium-sized enterprises due to missing expertise. Another topic that Zurbrügg rated to be in the top three challenges is the cross linkage of sites. Building stable and fast VPN connections is a prerequisite for the business but also brings dependencies that have to be considered. Last but not least, Zurbrügg states that mobile access to company resources is getting more popular and the infrastructure has to be made ready for this change. In order to do so, Zurbrügg does not exclude the option of cloud computing which brings great advantages in availability and performance. However, there are still some security concerns that prevent the immediate implementation.

Findings of the Interview with Hugo Bosshard, Studerus AG

Studerus is a small company with 55 employees based in Schwerzenbach, Switzerland. Its core business is the distribution of networking products and services. Their internal IT department consists of three employees and the interviewee, Hugo Bosshard, is the head of the IT department.

In the following, a short extract of the interview is provided:

> *"Requirements that are posed against IT in small and medium-sized enterprises are equal to the requirements that are common in large companies."* (Bosshard H. , 2012)

Bosshard states that the end-user requirements concerning IT are similar to those in large enterprises. Also small companies want to offer remote access solutions to their field representatives or have their infrastructure protected against security threats in an appropriate way. The problem is that small and medium-sized enterprises usually do not have enough financial and human resources to ensure equivalent service quality. It is therefore important that IT processes are automated wherever possible in order to reduce human interaction. A big advantage that small and medium-sized enterprises experience in general is that the employees usually have stronger commitment to the company.

> *"The conservation of internal IT knowledge is difficult to manage. The origin of this situation is a generation-problem. In the early days, nobody wanted to take care about IT. Nowadays, IT has such significance that knowledge management becomes crucial for the daily operations."* (Bosshard H. , 2012)

At Studerus, documentation of knowledge has a high significance. Bosshard admits that it is difficult to claim proper and actual documentation of the IT processes. He draws attention to the fact that it is important to keep the knowledge-management process simple. He does not prescribe documentation standards and says that it is much more important that the information is stored somewhere, regardless of the documentation format.

"Functioning backup and recovery processes are the hallmark of excellence for any IT department. The IT department loses its credibility if not even this core service is provided at a satisfactory level."

(Bosshard H. , 2012)

At Studerus, backup and recovery is considered to be the most important process within IT. Backup jobs are controlled regularly and restore tests are also scheduled from time to time.

The following topics were mentioned as the top-three challenges in the future:

- Home or remote office
- Security concerns
- Fast pace of IT

Employees want to have access to the company information from everywhere and all the time. This ubiquity brings big challenges regarding the security and availability of information. Malware becomes more intricate from day to day and security devices must adapt to these challenges. This challenge becomes even greater significance if the first challenge, home or remote office, is taken into account. It is no longer sufficient to install basic firewall mechanisms on the premises. The network protection must take place on each end-user device. Technologies are changing at always shorter cycles. Companies have to keep pace with this progress and especially for small and medium-sized enterprises this is hard to accomplish.

2.2 Conclusion

Valuable input can be taken from the results of the survey. The rated importance of the respective IT processes has crucial influence to the structure of the framework. The findings of the survey clearly indicate that operational processes like backup and security are very important. The design of the framework takes these results into consideration.

An important finding of the interviews is that the uniqueness of small and medium enterprises. This diversity of requirements has led to the necessity of the implementation of an assessment and thereby assuring a risk-based approach. Companies want to decide on their own what IT processes they want to improve and where to start when implementing IT governance. Therefore, a simple and quick assessment of the current maturity-level would be an ideal starting point.

The shortage of human IT resources seems to be omnipresent. Small and medium-sized enterprises have to focus on the core business and often, the significance of IT is underestimated. This situation especially counts for small enterprises where a lot of times IT is delegated to the employee with the best IT skills that is running the companies IT besides his daily business. This imbalance even becomes graver by having a look at the requirements that are posed against IT. As described in the findings of the interview with Hugo Bosshard (Interview Studerus AG, 2012), the requirements do not vary that much from the requirements that are posed against large companies. The framework should therefore provide simple governance guidance and be easily understandable. The goal must be that also non-IT employees understand the purpose and the structure of the framework and that the framework can be implemented without bringing in external consultants. A proper implementation of the framework should then ensure stable operations improve the management of IT resources.

The discussions with the interview participants about the IT topics and the future challenges of an IT department provide input for the composition of the processes. They help to determine the granularity of each process but also substantiate the findings of the survey.

V. The Framework

This IT Governance framework is tailored for the application within small and medium-sized enterprises. The main purpose of the framework is to improve IT governance activities within small and medium-sized enterprises by providing a generic framework including implementation guidance.

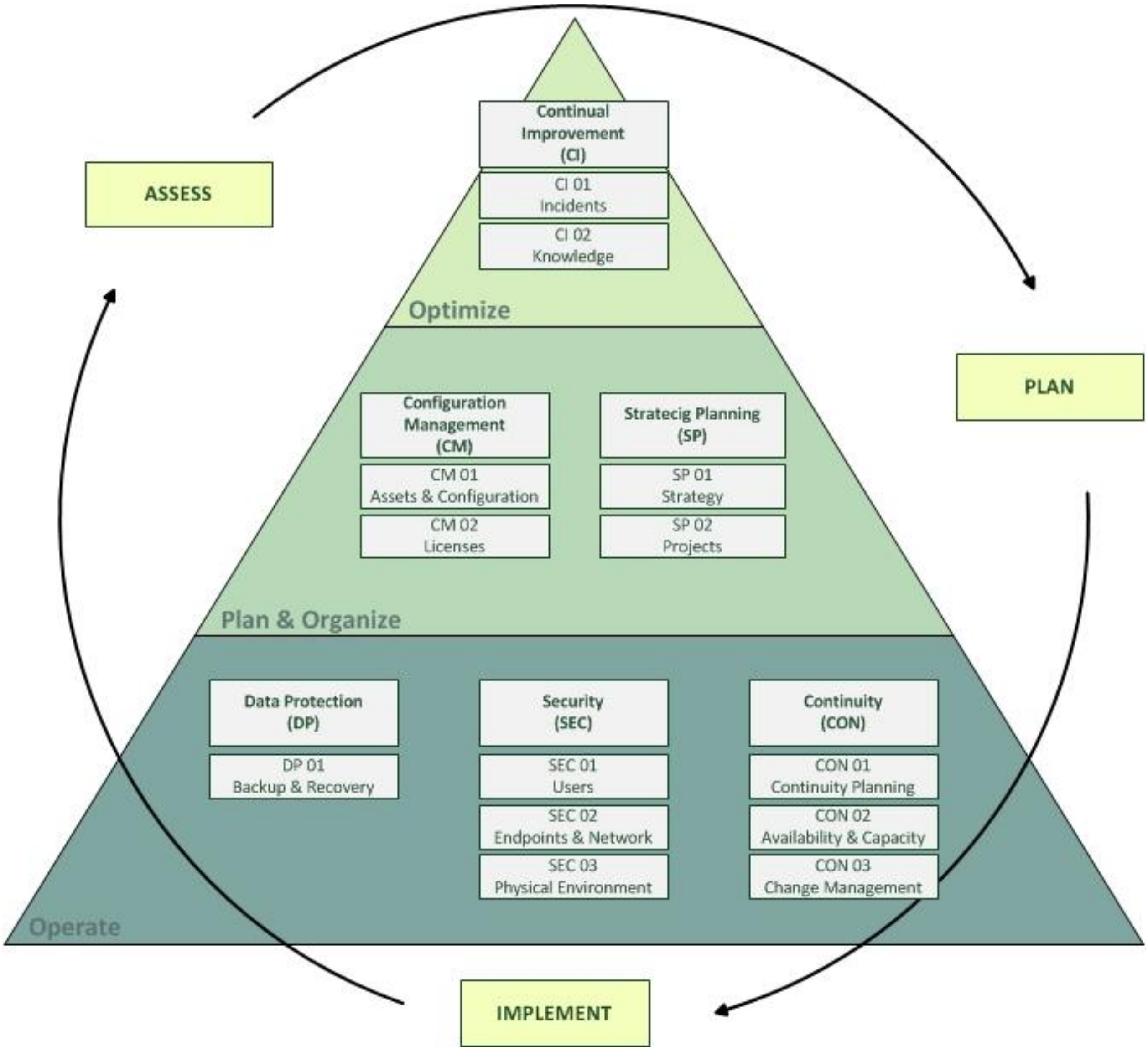


Figure 23: The framework.

1. Principles

The principles outline the characteristics of the framework and determine the scope of the framework regarding the applicability and the operational area.

1.1 Self-Empowerment

The framework is simple and easy to understand. This makes it possible that the implementation can be made by the company on its own, without special knowledge or external consulting necessary. The framework comes with a built-in lifecycle and an assessment which facilitates the implementation process by providing a step-by-step guidance.

1.2 Lightweight Approach

A framework should not be implemented for its own sake but should improve the overall maturity and quality of the related IT processes. Therefore, this framework is based on a lightweight approach meaning that no excessive requirements regarding the deliverables are prescribed.

The design of the framework is structured in a way that it fits well into the existing structures and processes. Although processes are proposed, it does not automatically mean that these processes have to be adopted in order to reach satisfactory results. The main objective of the segmentation into processes is that the described tasks are logically structured and can be assigned to an existing role or person in the company.

1.3 Compatibility

Since there are already numerous frameworks in the area of IT Governance, it is not reasonable to develop a distinct framework. This Framework is based on COBIT 5, but has been tailored for the needs for small and medium-sized enterprises. This approach ensures compatibility and extendibility. Companies that have implemented this framework can easily upgrade to COBIT 5 by consulting the provided COBIT 5 mapping in chapter 5.3. The mapping reveals the COBIT 5 processes that are included in this framework.

2. Components

The framework is divided into three layers, depicted in in a pyramid. The layers separate the domains regarding their importance for a company master the daily business. The form of the pyramid graphically expresses the level of importance that the layer has regarding to master the daily business.

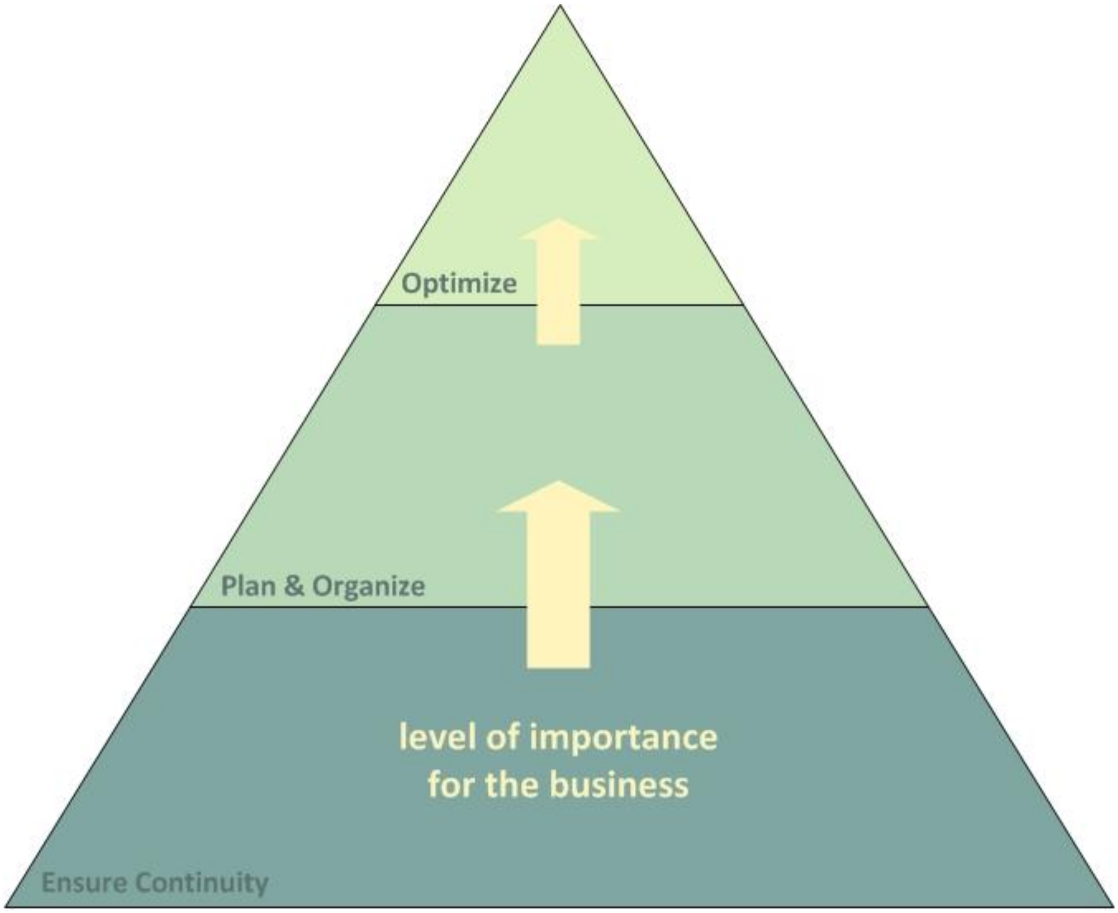


Figure 24: Explanation of layers.

Usually, incidents at the bottom layer have great impact on daily business processes. Running backup and recovery processes or a well-protected infrastructure is vital for the business. The layer Ensure Continuity contains all key processes that are necessary for solid and stable provisioning of IT services. The middle layer consolidates the planning and administrative tasks. Its main purpose is that IT services are effectively managed and that IT divisions move from reactive to proactive management. Optimization within the IT department is the intention of the top layer.

The domains are logically detached and the processes within the domains illustrate real-live processes in a common IT operations department, based on a functional separation.

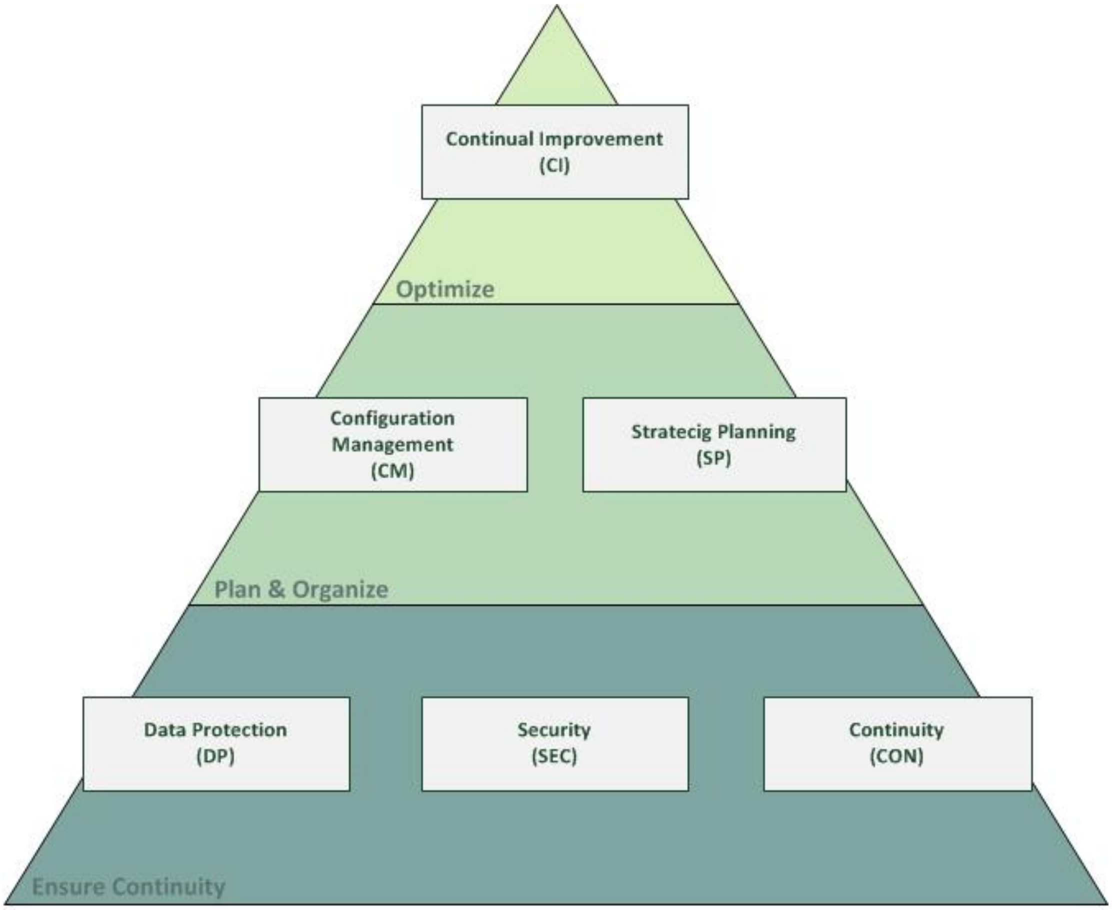


Figure 25: Explanation of domains.

In the following, each process is described in detail. Every process consists of a process goal, enumeration and explanation of tasks and prescribes the necessary attributes that should be produced or maintained. To enable monitoring functionalities, each process provides metrics that can be traced. Additionally, best practices are provided.

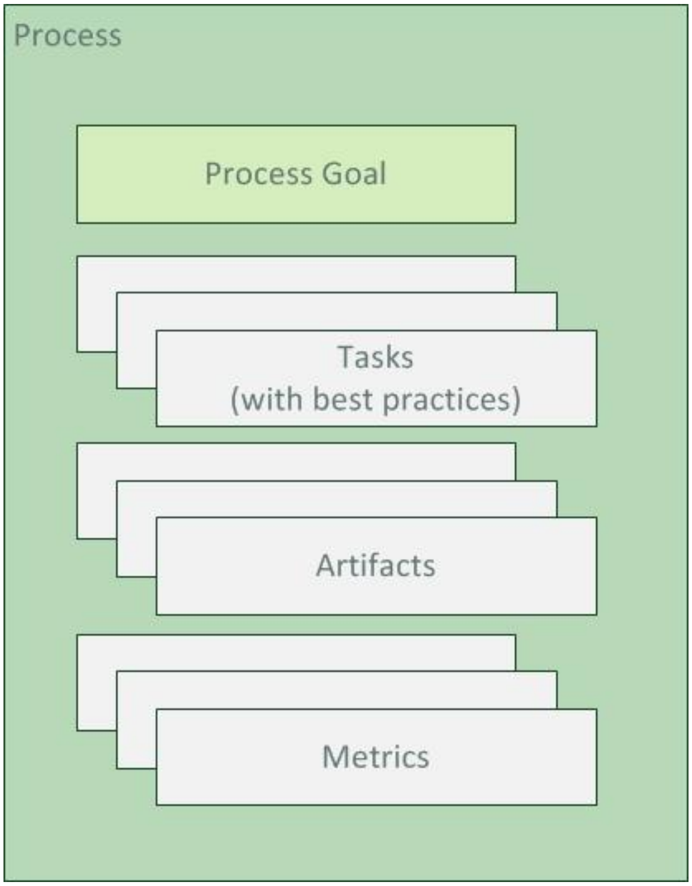


Figure 26: Structure of a process.

3. Processes

As already mentioned, this framework is tailored out of COBIT 5 for the needs of small and medium-sized enterprises. The content of the processes has been mainly taken out of the respective COBIT 5 processes (see the provided mapping in chapter 5.3). Where necessary, some minor changings have been made.

3.1 DP01: Backup and Recovery

3.1.1 Process Goal

Secure corporate data and ensure fast and efficient data recovery

3.1.2 Tasks

DP01.T01 Backup

Backup systems, applications, data and documentation according to a defined schedule. The following considerations should be taken into account:

- Frequency (monthly, weekly, daily etc.)
- Mode of backup (e.g., disk mirroring for real-time backups , DVD for long-term retention)
- Type of backup (e.g., full vs. incremental)
- Type of media
- Creation of logs
- Monitoring and alerting
- Physical and logical location of data sources
- Security and access rights
- Encryption

Best Practice

- Systems are usually backed up by creating images whereas data is backed up with file-based backup routines. It is common to apply a grandfather-father-son backup policy for most backup objects. This backup technique stores full copies of the backup source on a monthly basis, incremental backups on a weekly basis and differential backups on a daily basis. This approach ensures that any state can be restored, depending on the retention policy.
- Backups should be stored on a secure location and ideally not the same location as the data source whilst ensuring a fast recovery processes. It is recommended to use dual-destination backup to encounter this challenge. Dual destination backup allows storing backup objects on two (physically separated) locations. The first location should be quickly accessible in case of recovery and the second location should satisfy the demand of a secure backup location (e.g. backup in the cloud or in another company site).
- Compliance with external laws and regulations must be adhered. Be aware that for some industries (e.g. health) there are special requirements for data retention.

DP01.T02 Test backup objects

Periodically test backup objects through validation and restoration trials.

Best Practice

- Validation and testing is a vital task to ensure the quality of the backup. It may happen that backup objects can’t be restored, for what reason ever, and proper and regular testing is essential to perceive this misconduct. Whilst the restoration testing of data is a rather trivial process, restoration testing of systems and applications is difficult because of the required peripheral system that is necessary to check the functionality. The setup of virtual system environments has proven to be an efficient way for restoration testing of systems and applications.

DP01.T03 Establish restoration routines

Ensure that in case of data loss staff is well trained in the recovery process. Minimal system downtime or data leakage should be aimed-at.

3.1.3 Artifacts

DP01.A01 Backup and Recovery Plan

The backup and recovery plan should entail:

- Documentation of the backup process and the backup routines (DP1.T01)
- Testing scenarios and testing plan (DP1.T02)
- Recovery plan (if necessary step-by-step instructions) for each backup object (DP1.T03)

3.1.4 Metrics

DP01.M01 Percent of backup files transferred and stored securely

DP01.M02 Frequency of tests

DP01.M03 Number of recovery exercises and tests that have achieved recovery objectives

3.2 SEC01: Users

3.2.1 Process Goal

Minimize the business impact of information security vulnerabilities and incidents caused by user misconduct.

3.2.2 Tasks

DSS01.T02User Security

Ensure that all users have information access rights in accordance with their business requirements. Ensure that users are aware of security issues and establish user guidelines.

Best Practice

- Maintain user access rights in accordance with business function and process requirements. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.
- Manage user access lifecycle from creation of user account, to modifications and deletion (especially with trainee-accounts) and perform regular management review of all accounts and related privileges.
- Clear policies help to improve the security standard and raise the security awareness. A user policy should provide helpful information for users on how to behave and how to deal with security threats.

3.2.3 Artifacts

SEC01.A01 User Policy

The user policy is an internal document that contains regulations. It should describe the desired behavior with the use of information technology as well as in case of incidents and problems.

3.2.4 Metrics

SEC01.M01	Percent of stakeholders who understand policies
SEC01.M02	Frequency of policies review and update
SEC01.M03	Number of accounts incompliant with the policy

3.3 SEC02: Endpoints and Network

3.3.1 Process Goal

Minimize the business impact of information security vulnerabilities and incidents caused by endpoints or network devices

3.3.2 Tasks

SEC02.T01 Endpoint Security

Implement and maintain preventive, detective and corrective measures in place across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, and spam) and ensure that endpoints are secure. Up-to-date virus software and proper patching on every endpoint are the core security measures.

Best Practice

- The management of malware solutions and system updates is centralized, enabling reporting functionalities that permit better pro- and reactive measures in case of a security incident.
- The hardening of endpoints is another useful security measure. The following reflections should be taken into account (not conclusive):
  - ✓ Configure operating systems in a secure manner (e.g. local administrator rights)
  - ✓ Implement device lockdown mechanisms.
  - ✓ Manage remote access and control. (e.g. VPN)
  - ✓ Provide physical protection of endpoint devices.
  - ✓ Dispose of endpoint devices securely.

SEC02.T02 Network Security

Use security measures and related management procedures to protect information over all methods of connectivity.

Best Practice

- Nowadays, network devices offer a wide range of possibilities to face cyber security. Unified Thread Management (UTM) has proven to be an efficient measure to protect the local network and has become affordable not only for large enterprises. The following principles should be adopted:
  - ✓ Allow only authorized devices to have access to corporate information and the enterprise network. Configure these devices to force password entry.
  - ✓ Implement network filtering mechanisms such as firewalls and intrusion detection software with appropriate policies to control inbound and outbound traffic.
  - ✓ Encrypt information in transit according to its (implicit or explicit) classification.
  - ✓ Apply approved security protocols to network connectivity.
  - ✓ Configure network equipment in a secure manner.
  - ✓ Carry out periodic penetration testing to determine adequacy of network protection.
  - ✓ Carry out periodic testing of system security to determine adequacy of system protection.

3.3.3 Artifacts

SEC02.A01 Security Plan for Endpoints and Network

The security plan should cover:

- The management of Endpoint Security (SEC02.T01)
- The management of Network Security (SEC02.T02)

3.3.4 Metrics

SEC02.M01	Number of vulnerabilities discovered
SEC02.M02	Number of outstanding patches at a point in time
SEC02.M03	Number of incidents involving endpoint devices
SEC02.M04	Number of security incidents causing business disruption

3.4 SEC03: Physical Environment

3.4.1 Process Goal

Protect the physical infrastructure against unauthorized access.

3.4.2 Tasks

SEC02.T01 Physical Security

Define and implement procedures to grant, limit and revoke access to IT systems according to business needs, including emergencies. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.

Best Practice

- Manage the requesting and granting of access to the computing facilities. Formal access requests are to be completed and authorized by management of the IT site, and the request records retained. The forms should specifically identify the areas to which the individual is granted access.
- Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities.
- Require visitors to be escorted at all times while onsite by a member of the IT operations group. This is hard to implement in small and medium-sized enterprises and depends on several factors (e.g. level of trust to the visitor, purpose of the task).
- Conduct regular physical security awareness training.

3.4.3 Artifacts

SEC03.A01 Security Plan for physical Security

The security plan for physical security should cover:

- The management of Physical Security (SEC03.T01)

3.4.4 Metrics

SEC03.M01 Number of physical-security related incidents

3.5 CON01: Continuity Planning

3.5.1 Process Goal

Ensure continuity of critical business operations.

3.5.2 Tasks

CON01.T01 Develop and implement a business continuity response

Identify it services that are critical to the business operations and implement rational continuity measures.

Best Practice

- Identify potential scenarios likely to give rise to events that could cause significant disruptive events. These events should then be classified regarding the time of disruption in case of failure and their importance. The importance is often determined through the maximal tolerable outage. The time required to recover should also be taken into consideration.
- Identify measures that will reduce the likelihood through prevention and determine cost-effective measures that are to be taken in case of an incident. These procedures should be well documented so that in case of a disruptive event, a structured course of action can be taken.
- Clear roles and responsibilities for each measure must exist.

CON01.T02 Exercise, test and review the business continuity plan

Test the continuity arrangements on a regular basis.

Best Practice

- The testing of the continuity plan has multiple purposes. First you want to be sure that the defined measures work as desired (verification). Secondly, staff is getting trained in dealing with exceptional situations (learning) and last but not least, the procedures can be optimized by accomplishing continuity tests (optimization).

3.5.3 Artifacts

CON01.A01 Continuity Plan

The continuity plan should contain:

- A business impact analysis with potential scenarios (CON01.T01)
- Incident response actions based on the continuity requirements(CON01.T01)
- Testing plan, containing the test objects and a time plan (CON01.T02)

3.5.4 Metrics

CON01.M01	Number of critical business systems not covered by the continuity plan
CON01.M02	Percent of successful business continuity incidents
CON01.M03	Number of planned business continuity exercises
CON01.M04	Percent of executed business continuity exercises that have achieved its objectives

3.6 CON02: Availability and Capacity

3.6.1 Process Goal

Maintain service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements.

3.6.2 Tasks

CON02.T01 Identify availability and capacity requirements

Balance current and future needs for availability, performance and capacity with cost-effective service provisioning.

Best Practice

- Assess availability, performance and capacity of it services and resources and determine the baselines. The assessment should consider the current and forecasted requirements. The following criteria should be considered:
  - ✓ Customer requirements
  - ✓ Business priorities and objectives
  - ✓ Budget impact
  - ✓ Resource utilization
  - ✓ IT capabilities and industry trends
- Ensure periodic monitoring (or where possible automated) and implement appropriate alerting functionalities (e.g. free disk space).
- Plan, prioritize availability, performance and capacity implications of changing business needs and service requirements.

3.6.3 Artifacts

CON02.A01 Availability and Capacity Plan

The availability and capacity plan should contain:

- Availability, performance and capacity baselines
- Monitoring and alerting configuration
- Action plan concerning availability and capacity for the next couple of years (depending on industry and procurement strategy)

3.6.4 Metrics

CON02.M01 Percent of unplanned capacity, performance or availability upgrades versus planned upgrades

CON02.M02 Number of availability incidents

CON02.M03 Number of events where capacity has exceeded planned limits

3.7 CON03: Change Management

3.7.1 Process Goal

Enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment.

3.7.2 Tasks

CON03.T01 Manage Changes

Evaluate, prioritize and authorize change requests. Implement standard change procedures and ensure proper monitoring and control mechanisms.

Best Practice

- Ensure that all changes are conducted in a structured way. The following considerations should be taken into account (a simple form is enough):
  - ✓ Impact assessment
  - ✓ Prioritization and authorization
  - ✓ Emergency changes,
  - ✓ Tracking
  - ✓ Reporting
  - ✓ Closure and documentation
- All changes should be coordinated centrally through one consistent person, so that holistic overview is ensured. This is vital to recognize possible dependencies.

CON03.T02 Prepare and execute Testing

Establish a test plan and required environments to test individual or integrated solution components, including the business processes and supporting services, applications and infrastructure. Execute testing continually based on the change plan.

Best Practice

- Suitable testing of scheduled changes helps to verify that the solution will operate successfully in the live environment and delivers the intended results.
- Create a test plan and ensure that the test procedures should simulate real-world conditions.
- For critical applications it is recommended to temporarily set up mirrored environments where the real environment can be simulated at a very high degree of similarity. Note that not everything can be simulated and that a certain residual risk will remain.
- Make sure that the test results are logged.

3.7.3 Artifacts

CON03.A01 Change Plan

The change plan should contain:

- Description of the change management process
- Overview about scheduled changes
- Reference to the required respectively demanded forms (change request, test plan)

3.7.4 Metrics

CON03.M01 Percent of unsuccessful changes due to inadequate impact assessments

CON03.M02 Percent of total changes that are emergency fixes

CON03.M03 Number of executed tests

3.8 CM01: Assets & Configuration

3.8.1 Process Goal

Account for all IT assets and optimize the value provided by these assets. Provide sufficient information about service assets to enable the service to be effectively managed

3.8.2 Tasks

CM01.T01 Identify and Manage Assets

Manage IT assets though their life cycle. Make sure that their use delivers value at optimal cost, they remain operational and physically protected.

Best Practice

- Identify all assets and maintain alignment with the change- and configuration management.
- Verify the existence of all owned assets by performing regular physical and logical inventory checks and reconciliation.
- Source, receive, verify, test and record all assets in a controlled manner, including physical labeling, as required.

CM01.T02 Manage the Configuration

Define and maintain descriptions and relationships between key resources and capabilities required to deliver IT-enabled services.

Best Practice

- Define and agree on the scope and level of detail for configuration management.
- Establish and maintain a logical model of the services, assets and infrastructure and how to record configuration items and the relationships amongst them. A good point to start is a drawing of the system landscape that proves a good overview by naturally selecting the level of detail.
- Periodically verify live configuration items against the configuration repository by comparing physical and logical configurations.

3.8.3 Artifacts

CM01.A01 Asset Register

The asset register should cover:

- List of all IT assets with information about procurement, maintenance and disposal (e.g. warranty information).

CM01.A02 Configuration Repository

The configuration repository should cover:

- Graphical abstraction of the system landscape
- Actual configuration of the selected configuration items
- Description of the relationship among the configuration items.

3.8.4 Metrics

CM01.M01	Number of assets not utilized
CM01.M02	Number of deviations between the configuration repository and live configuration

3.9 CM02: Licenses

3.9.1 Process Goal

Ensure that licenses are procured in the right quantity.

3.9.2 Tasks

CM02.T01 Manage Licenses

Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage.

Best Practice

- Maintain a register of all purchased software licenses and associated licenses agreements.
- On a regular basis, conduct an audit to identify all instances of installed licensed software. Decide whether there is a need to retain or terminate licenses in case of dissimilarities.

3.9.3 Artifacts

CM02.A01 License Register

The license register should cover:

- The management of software licenses (contact information, license keys and agreements)
- An actual overview about the current status

3.9.4 Metrics

CM02.M01	Percent of used licenses against paid-for licenses

3.10 SP 01: Strategy

3.10.1 Process Goal

Align IT with business objectives.

3.10.2 Tasks

SP01.T01 Determine IT direction

Provide a holistic view of the current business and IT environment and the future direction.

Best Practice

- Consider the current enterprise environment and business processes, as well as the external environment of the enterprise (industry drivers, relevant regulations, basis for competition) for the future direction.
- Identify key stakeholders and obtain insight on their requirements. Then, identify and analyze sources of change in the enterprise and ascertain priorities.
- Make sure that the future direction is controlled / revised regularly

SP01.T02 Define and communicate road map

Develop initiatives and communicate to the stakeholders.

Best Practice

- Define a road map based on the results of SP01.T01. Determine dependencies, overlaps, synergies and impacts amongst initiatives.
- Identify resource requirements, schedule budgets for each of the initiatives.

3.10.3 Artifacts

SP01.A01 Road Map

The road map is the strategy document regarding IT decisions. The road map should cover:

- Statement about the future direction
- Initiatives to be performed embedded in a chronology

3.10.4 Metrics

SP01.M01	Percent of projects that can be directly traced back to the strategy
SP01.M02	Frequency of updates to the road map

3.11 SP02: Projects

3.11.1 Process Goal

Optimize the performance of IT-projects in response to changing enterprise priorities and demands.

3.11.2 Tasks

SP02.T01 Maintain the IT-Portfolio

Maintain portfolio of projects, IT services and IT assets.

Best Practice

- Create and maintain portfolios of IT-enabled investment programs, IT services and IT assets, which form the basis for the current IT budget and support the road map.
- On a regular basis, monitor and optimize the performance of the IT-portfolio to exploit synergies, eliminate duplication between programs and identify and mitigate risk.

SP02.T02 Manage projects

Maintain a standard approach for project management. Plan and monitor IT projects.

Best Practice

- Enforce a standard approach for project management (e.g. Hermes (Schweizerische Eidgenossenschaft, 2005), PMBoK (Project Management Institute, 2009)). Ensure that the approach covers the full life cycle.
- Establish and maintain project planning to guide project execution and control throughout the life of the project.
- Ensure that milestones are accompanied by significant deliverables requiring review and sign-off.

3.11.3 Artifacts

SP02.A01 IT-Portfolio

The IT-Portfolio should cover:

- Consolidation of all current IT initiatives
- Guidelines for projects (e.g. procedure model)
- Monitoring and control mechanisms for projects

3.11.4 Metrics

SP02.M01	Number of running initiatives
SP02.M02	Percent of successful initiatives
SP02.M03	Percent of projects undertaken without approved business cases
SP02.M04	Percent of deviations from the project plan

3.12 CI01: Incidents

3.12.1 Process Goal

Achieve increased productivity and minimize disruptions through quick resolution of user queries and incidents. Increase availability, reduce costs and improve customer convenience and satisfaction by reducing the number of operational problems.

3.12.2 Tasks

CI01.T01 Manage Incidents

Provide timely and effective response to user requests and resolution of all types of incidents.

Best Practice

- Implement an incident register (e.g. ticketing system)
- Define incident and service request classification and prioritization schemes to ensure consistent approaches for handling, informing users about and conducting trend analysis.
- Define appropriate support groups to assist with identification, root cause analysis and solution determination. Define priority levels through consultation with the business and report the status of identified incidents.
- Make sure that known-errors are recorded and communicated.

3.12.3 Artifacts

CI01.A01 Incident Register

The incident register should cover:

- Incident management procedures
- All incident requests
- Known errors

3.12.4 Metrics

CI01.M01 Number of incidents causing disruption to business-critical processes

3.13 CI 02: Knowledge

3.13.1 Process Goal

Provide the IT-related knowledge required to support all staff in their work activities and for informed decision making and enhanced productivity.

3.13.2 Tasks

CI02.T01 Manage IT-Knowledge

Maintain the availability of relevant, current, validated and reliable knowledge to support all process activities and to facilitate decision making. Plan for the identification, gathering, organizing, maintaining, use and retirement of knowledge.

Best Practice

- Establish and maintain a knowledge database (e.g. Wiki). Define documentation standards.
- Ensure user training and increase user awareness through training and sensitization.

3.13.3 Artifacts

CI02.A01 Knowledge Database

The Knowledge Data base must be able to:

- Document unstructured information and transform it to knowledge.
- Publish and make knowledge accessible to relevant stakeholders.

3.13.4 Metrics

CI02.M01	Level of satisfaction of users
CI02.M02	Frequency of updates in the knowledge database
CI02.M03	Percent of knowledge repository used

4. Lifecycle

The lifecycle provides good guidance for implementing the framework. It is based on a continual improvement process where first, the current situation is assessed, then the desired state is defined and the necessary measures are taken. In the last step of the cycle, the defined initiatives are implemented.

The following premises should be taken into consideration.

- IT governance cannot be implemented within a big-bang approach but needs to emerge slow and steadily.
- A governance-aware enterprise culture is the foundation for successful implementation.
- Management support is vital for the success.
- Provided that these preconditions are covered, implementation proposals can begin.

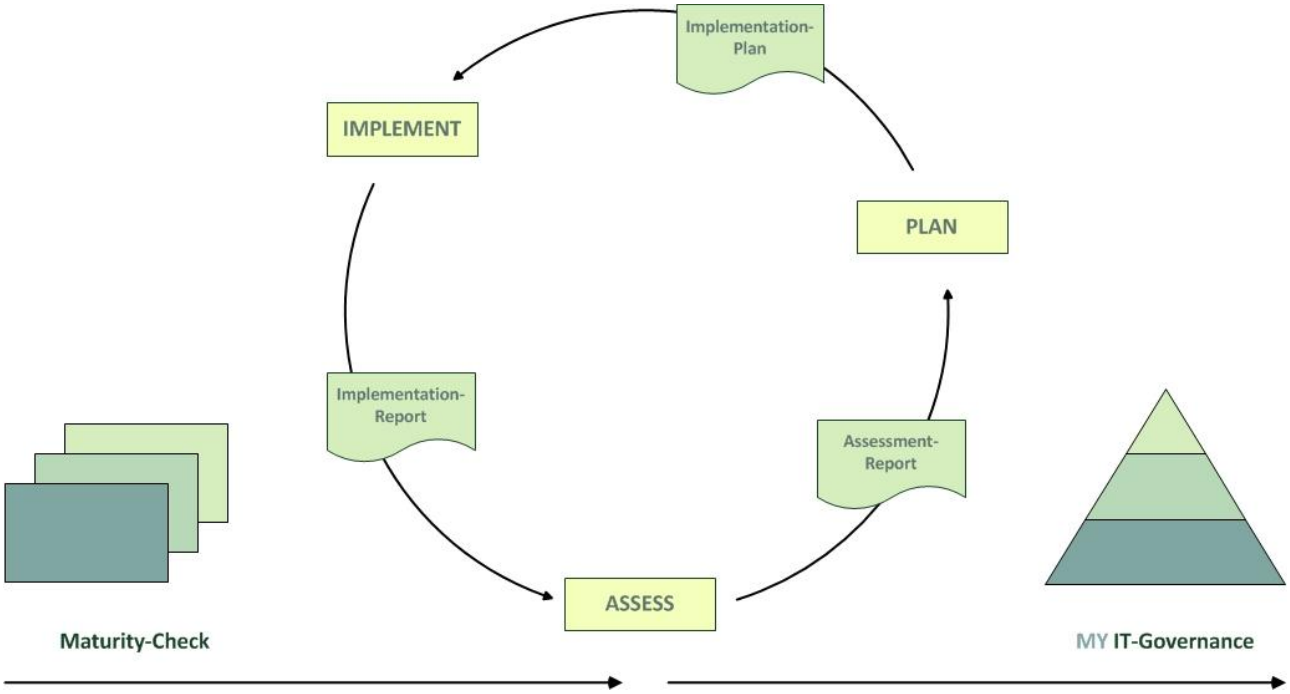


Figure 27: Lifecycle.

4.1 Assess

The primary goal of the assessment phase is to conduct an analysis of the current maturity regarding IT governance tasks. The maturity-check provided within the framework (it-governance-for-sme.ch/maturity-check) offers an easy way to initially assess the current situation. It is also helpful because by replying the questionnaire all relevant IT topics pop up and the assessor automatically becomes confronted with practically relevant interrogations. In the best case the accomplishment of the maturity-check not only helps to determine the actual state but already sensitizes the company regarding the most important IT governance topics. Another advantage of the maturity-check is that the assessor already starts working with the framework and thereby learns to know the structure of the framework from the bottom. The following picture illustrates the result of an example assessment. Each process is filled with the respective color that was calculated from the indications of the questionnaire. Red means that the assessed process maturity is insufficient, orange indicates a little better process maturity and the light green states that the process maturity is sufficient but there is still some room for improvement. The dark green means that the process is implemented with a high process maturity.

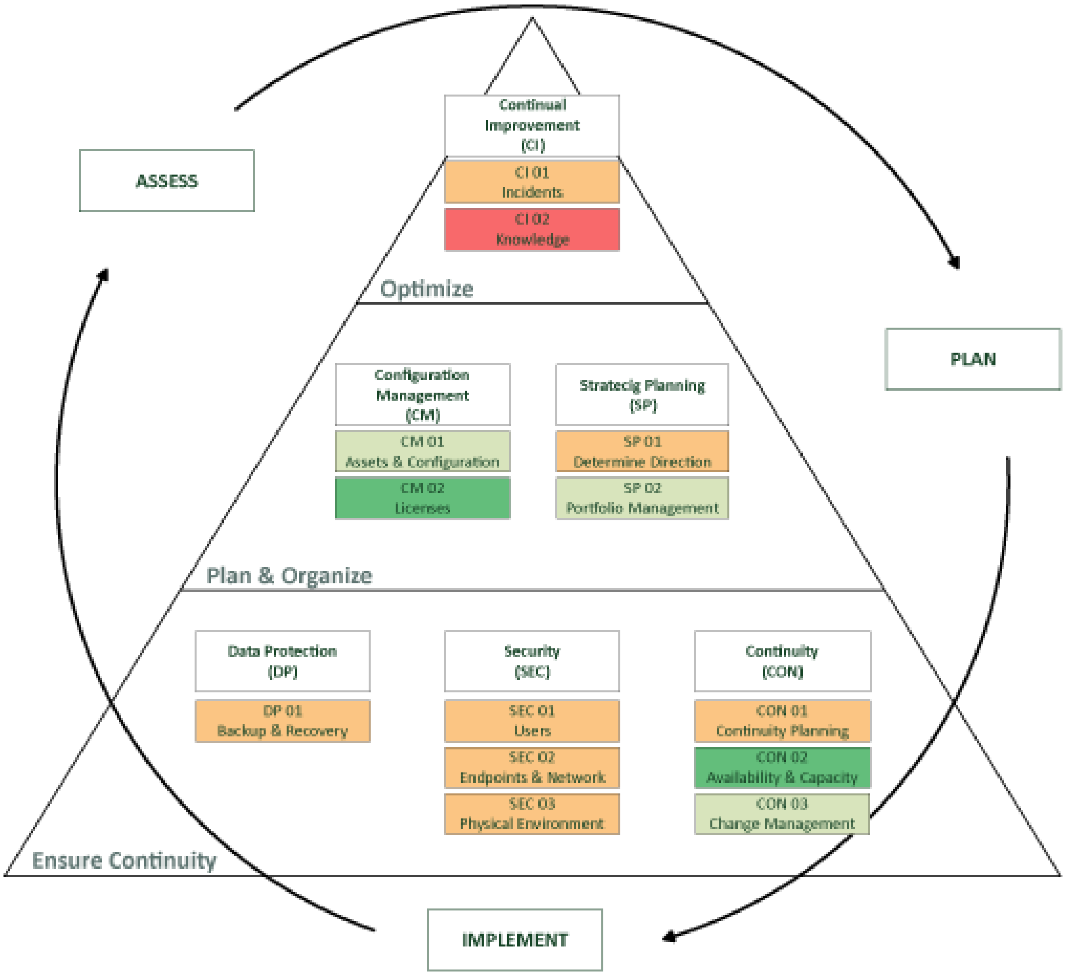

ASSESS
PLAN
IMPLEMENT
Continual Improvement (CI)
CI 01 Incidents
CI 02 Knowledge
Optimize
Configuration Management (CM)
CM 01 Assets & Configuration
CM 02 Licenses
Stratecig Planning (SP)
SP 01 Determine Direction
SP 02 Portfolio Management
Plan & Organize
Data Protection (DP)
DP 01 Backup & Recovery
Security (SEC)
SEC 01 Users
SEC 02 Endpoints & Network
SEC 03 Physical Environment
Continuity (CON)
CON 01 Continuity Planning
CON 02 Availability & Capacity
CON 03 Change Management
Ensure Continuity

Figure 28: Result of example assessment (on it-governance-for-sme.ch).

Once the maturity-check is done, the results must be analyzed. It is therefore vital to study the framework and the proposed tasks, artifacts and metrics and already trying to make some linkage between the framework and the real-life situation.

An assessment-report is the final delivery of this phase. It contains the findings from the maturity-check as well as the subsequent analysis. The main purpose of this document is that the weaknesses are clearly addressed so that it can serve as a base for decision making.

4.1.1 Artifact

Assessment-Report

4.2 Plan

In the planning phase, the desired state is defined and, with help of the assessment-report, an implementation plan is set up. It is of great importance that the desired result is clear to everyone. The desired result can be expressed with help of the assessment-report and the described artifacts in the framework.

The implementation plan should consolidate all scheduled activities. For all activities, the following information must be provided:

- Goal
- Priority
- Result (e.g. process or artifact)
- Time horizon
- Responsible person(s)
- Estimated implementation cost
- Estimation of required manpower

This proceeding ensures a structured approach and enables monitoring and control of the implementation progress. Prioritization should be with regards to the severity of the discovered weakness during the assessment phase and the estimated overall expenditures. After the implementation-plan is elaborated, it must be reviewed and approved by the management.

4.2.1 Artifact

Implementation-Plan

4.3 Implement

The implementation consists of the three main steps execute, monitor and review. The execution of the activities happen according to the implementation plan and regular monitoring activities ensure the implementation success. After completion, the result of the activity is reviewed and an overall implementation-report concludes the implementation phase.

4.3.1 Artifact

Implementation-Report

5. Benefits

This chapter lists the benefits for small and medium-sized enterprises of using this framework.

5.1 Usability

This framework has been specifically developed for small and medium-sized enterprises. Whereas the content within the prescribed processes is tailored from COBIT 5 and therefore does not differ much (where an equivalent process is existent in this framework), organizational recommendations such as roles and responsibilities or the implementation guidance have not been adopted. Just from a rational perspective it would not be reasonable to apply the provided roles and responsibilities from COBIT. The organization of small and medium-sized enterprises simply does not allow such a setup. This framework does not provide any role or responsibility. The company is absolutely free in deciding its organizational structure and the framework can be implemented regardless of the organizational and operational structure. Although COBIT does not prescribe an organizational structure by defining the roles and responsibilities, the quantity of the described roles make an implementation within a small and medium-sized enterprise nearly impossible. The lightweight design of this framework enables maximal flexibility.

As described in the framework’s principles, self-empowerment is another important factor that determines the usability of the framework. The framework is structured in a simple and reasonable way and is easily understandable. The simplicity of the structure is necessary for ensuring this self-empowerment approach. A company should be able to set up this IT governance framework without external help. Furthermore, the company should feel equal to manage the prescribed processes after successful implementation. An IT governance initiative should not be started for its own sake but for the sake of improving the IT processes. Therefore it is vital for any enterprise that the processes of this framework become an integral part of the IT organization.

5.2 Compliance

Compliance with external laws and regulations can be improved by applying this framework. It does not mean that the framework solves all challenges regarding compliance but the better each process is implemented, the more probable it is that the compliance requirements are fulfilled. According to Grünendahl et al. (Das IT-Gesetz: Compliance in der IT-Sicherheit, 2012, p. 13), IT governance helps to improve the awareness regarding IT compliance issues. Additionally, clearly structured IT processes provide a good overview across the IT landscape which eases to address compliance topics.

5.3 Compatibility with COBIT 5

The framework is based on COBIT 5. Although compliance with COBIT 5 is not a direct advantage that argues for the application of this framework, it may be beneficial to first adopt this framework than directly applying COBIT 5. The implementation of COBIT 5 takes much more personal, organizational and financial resources. The advantage emerges when an enterprise that actually has this framework in place wants to upgrade to COBIT 5. All processes in this framework can be mapped to the COBIT 5 enabling processes (ISACA, 2012) assuring upwards compatibility.

The following figure maps the processes within this framework with COBIT 5.

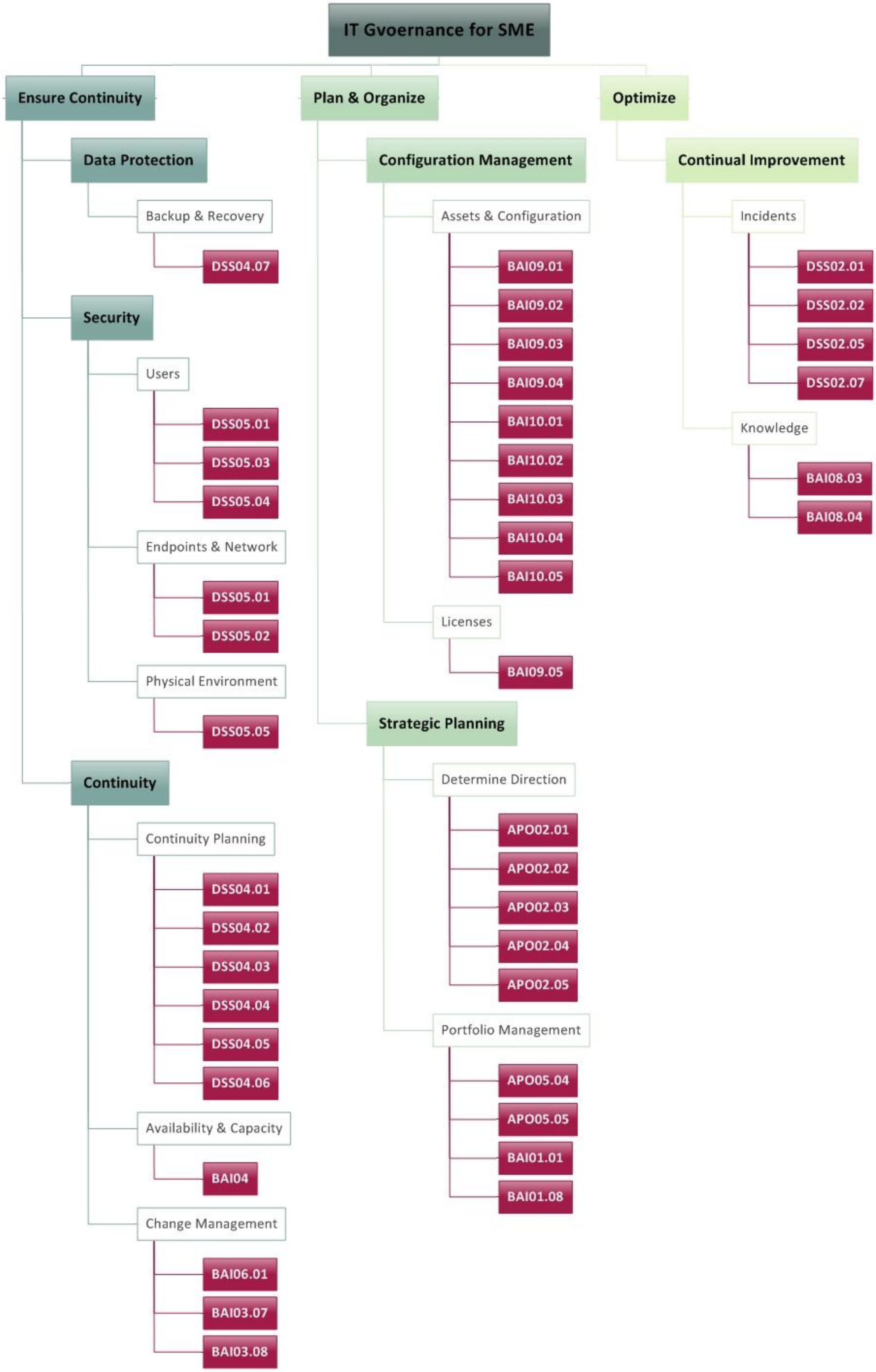


Figure 29: Mapping to COBIT 5.

5.4 Holism

IT governance can be considered to be the rooftop of all IT processes within the enterprise. It is therefore important that an IT governance initiative covers all relevant aspects of IT.

The IT governance focus areas defined by the IT Governance Institute (IT Governance Institute & KPMG, 2003) provide a solid overview by enlisting the relevant parts of IT governance. The focus areas are introduced in chapter II and the following table contains a mapping between the processes prescribed in the framework and the IT governance focus areas.

The respective color indicates the level of affiliation of the process to the IT governance focus area. Grey means that there is no substantial coherence; the bright green indicates that the area is partially or indirectly covered and the dark green signifies direct coverage of the focus area.

	Strategic Alignment	**Value Delivery**	**Risk Management**	**Resource Management**	**Performance Measurement**
DP01 **Backup & Recovery**		Solid backup and recovery policies fasten disaster recovery.	Risk management process is part of the backup and recovery plan.	Data and Applications are crucial IT key factors.	
SEC01 **Users**		Good user security provides indirect value through prevented incidents.	The security plan implies the risk management for user security.	Staff is affected by the security plan.	
SEC02 **Endpoints & Network**		Good endpoint and network security provides indirect value through prevented incidents.	The security plan implies the risk management for endpoint and network security.	Endpoints and Network devices (Technology) are securely configured and managed.	
SEC03 **Physical Environment**		A well protected physical infrastructure prevents from theft and misconfiguration.	The security plan implies risk management for the physical infrastructure.	Facilities are properly managed.	
CON01 **Continuity Planning**		Disruptive events are reduced.	Risk management practices are applied by establishing the		

	Strategic Alignment	Value Delivery	Risk Management	Resource Management	Performance Measurement
			business impact.		
CON02 **Availability & Capacity**	Future needs regarding availability and capacity are taken into account.	Optimal and cost-effective service provisioning.	Proactive risk management through monitoring and alerting.		
CON03 **Change Management**		Improved flexibility and agility.	Risk is reduced through proper testing		
CM01 **Assets & Configuration**		Rational sourcing		All IT assets are properly managed and configured.	
CM02 **Licenses**		Effective and efficient procurement		Software licenses are centrally managed	
SP01 **Strategy**	Optimal alignment with business objectives and long-term IT goals	Future direction is clear which leads to a concentration of resources to the determined direction			
SP02 **Projects**		Exploit synergies and reduce redundancies		IT Portfolio management of programs, projects, services and assets	
CI01 **Incidents**		Optimal end-user support increases productivity			
CI02 **Knowledge**		Knowledge-Database enhances productivity		Transformation of information into knowledge.	

Table 7: Coverage of IT governance focus areas.

The table states that all focus areas are covered by the framework, except performance measurement. Although performance measurement is not directly addressed, the defined metrics within the processes provide the foundation for setting up concrete measures for assessing the performance. However, a direct coverage of this focus area is indeed inexistent. This is due to the fact that performance measurement was not rated to be that important in the interviews so that it should have been integrated in the framework. A reason for this may be that the ability to measure the performance requires a certain process maturity (repeatability) and, at most of the interview partners, this maturity level was still far away.

This framework should enable small and medium-sized enterprises to govern their IT in a simple and pragmatic manner. By looking at the table, this statement can be confirmed. Rather strategic topics have been reduced to an adequate minimum and special emphasis has been placed to operational topics. To summarize, the framework covers all relevant IT processes for small and medium-sized enterprises and its implementation is a good step towards IT governance.

VI. Testing of the Hypothesis

The review and testing phase serves the purpose of verification and validation. With reviews of industry experts, the framework becomes verified regarding its completeness and consistence. The validation is conducted in order to prove the underlying hypothesis and to gain a first reaction of potential users.

1. Testimonial by Peter Bitterli, Bitterli Consulting AG

Peter R. Bitterli (Dipl. Math. ETH; CISA, CISM, CGEIT) is the owner of Bitterli Consulting AG, an IT auditing and consulting company. He is also member of the executive board of the ISACA Switzerland Chapter and is responsible for the education. Peter R. Bitterli is the publisher of the "COBIT Praxishandbuch (Bitterli, Praxishandbuch COBIT, 2006)" and many other articles on IT governance.

1.1 Testimonial

"Take a Step Towards Governance of Enterprise IT - Getting a return on investment in information technology and managing the related risks can be a tremendous challenge for almost any company. Because of their limited (personal) resources, this is especially true for small to medium-sized enterprises (SME) as they often lack the governance functions such as steering committees, project offices and other resources that the larger companies have.

Implementing (IT) governance in such organisations is, therefore, not an easy task – especially as most of the existing management and governance frameworks are not really geared to the special requirements of small enterprises. An IT governance framework "reduced to the max" is a highly interesting option that would bring the task of governance and management of enterprise IT into the reach of SME.

The IT governance framework presented in the thesis of Peter Josi has been specifically geared towards SME. Based on COBIT 5 but reduced to 13 processes grouped into 6 domains in a life cycle approach, Josi's framework can most probably be implemented even by rather small companies. The best practices shown in the framework for each of the processes are well chosen and certainly important for SME. And having metrics for measuring the actual state and defining the target state for each of the processes is a sound idea as this will help to implement the IT governance framework. However, the metrics provided should be improved as some of them don't really comply with the well-known SMART requirements for measurements. But the examples shown will give you an indication of the measurement approach to take and can be a basis for defining your own, enterprise-specific metrics.

Governance ensures that stakeholder needs and requirements are used to set direction and prioritise actions – although these governance tasks are also important for SME, they are not much represented in Josi's framework. When looking at the listed processes in more detail, one can clearly see that they mostly correspond to management and not to governance tasks: The majority of the processes in the framework are for planning, building, running and monitoring IT-related activities. "Only" the two processes SP01 (Determine IT Direction) and SP02 (Portfolio Management) represent the strategic planning part of Josi's framework and by this the governance aspects.

Nevertheless: having a sound management basis in place is a prerequisite for successful governance activities – in that sense, the seeming imbalance in Josi's framework enable SME to focus their limited resources. And – as a matter of fact – only 5 of the 37 processes in the "original" COBIT 5 framework are directly governance-related, too.

I urge responsible persons in SME to check the validity of Josi's approach to management and governance of enterprise IT." (Bitterli, Testimonial, 2012)

2. Testimonial by Prof. Dr. Christian Thiel, FHSG

Prof. Dr. Christian Thiel is an IT governance expert with both, practical as well as theoretical experience. He currently teaches at the University Of Applied Sciences Of St. Gallen at the institute of information- and process-management. From 2001 – 2008, Prof. Thiel was chief information security officer at Raiffaisen Switzerland.

2.1 Testimonial:

"Die IT ist heute ein fester Bestandteil jeder Organisation und hat die betrieblichen Prozesse massgeblich verändert. Die IT unterstützt Firmen in ihrer gesamten Wertschöpfungskette und hat daher einen wesentlichen Einfluss auf deren Wettbewerbsfähigkeit, sei dies durch Verbesserung der Produktivität, Erhöhung der Kosteneffizienz oder Anstieg der Qualitätsniveaus von Produkten. Geschäftsleitungsmitglieder und Verwaltungsräte werden daher immer häufiger mit der Frage konfrontiert, ob ihre eigene Informatik in der Lage ist, die aktuellen und zukünftigen Bedürfnisse des Unternehmens zu erfüllen. Dabei scheint der Schlüssel zu einer profitablen und wirkungsvollen IT in deren Führung und Steuerung zu liegen – also in der IT Governance. Es existieren denn auch verschiedene Referenzmodelle für IT-Governance, allen voran COBIT und ITIL sowie Empfehlungen des IT Governance Institute.

Betrachtet man diese genauer, sind es in etwa 20 Aufgaben, welche ein Unternehmen auf einer genügend hohen Maturitätsstufe betreiben muss. Diese Kernaufgaben reichen vom stabilen Betrieb über ausreichende Datensicherung bis zur physischen und technischen Sicherheit – und vom konsequenten Testen von selbstentwickelten oder eingekauften Anwendungen bis zur Implementierung einer mittels Zugriffsschutzsystemen unterstützten, ausreichenden Funktionentrennung im Fachbereich wie in der IT. Besondere Aufmerksamkeit benötigen Aufgaben wie (IT-) Risikomanagement, Compliance oder auch Outsourcing; ein Thema, an dem kaum ein KMU vorbeikommt.

Studien zeigen (z.B. Diplomarbeit von Christian Landolt, Uni Zürich, Lohnt sich IT-Governance auch für KMUs? Juli 2009, bzw. IT-Governance – auch für KMU notwendig und sinnvoll, von Peter Bitterli, ISACA-Newsletter Nr.01, März 2011) zeigen auch bei KMU einen klaren Bedarf an IT-Governance auf, wobei aber eine Umsetzung von sämtlichen z.B. im COBIT-Framework aufgeführten Faktoren viel zu aufwändig und für ein KMU weder durchführbar noch sinnvoll ist. Eine Fokussierung auf wenige Themen ist daher notwendig.

Ältere Ansätze zu einer Fokussierung basierend auf früheren COBIT Versionen finden sich z.B. im COBIT@Quickstart, 2nd Edition 2007 des IT Governance Institute. Nach der mehrfachen Überarbeitung und Aktualisierung des COBIT Frameworks hin zur Version 5 bedarf es auch hier einer grundlegenden

Erneuerung, wie sie z.B. in IT Governance for SME, A Framework, von Peter Josi angegangen wird. Dieses Framework arbeitet mit 21 Tasks (vergleiche oben; 20 Aufgaben) und reduziert damit im Vergleich zu COBIT 5 den Implementierungsaufwand erheblich. Die Aufteilung in 3 Layers ist nachvollziehbar (wobei sie nur eine verkürzte Dartstellung des PDCA Zyklus ist) und steigert die Übersichtlichkeit. Die im Kapitel 1 genannten Príncipes können mit dem Framework erreicht werden (wobei speziell bei 1.4 eine Begründung fehlt, warum Compliance erreicht werden kann)

Weitere Anmerkungen:

- *Ein wichtiger Punkt gerade für KMU ist das Thema Outsourcing bzw. allgemein Unterstützung durch externe Partner. Diesen Punkt - vor allem das Thema SLA - sollte man m.E. in das Framework aufnehmen.*
- *Auch wenn sich das Framework stark an COBIT 5 anlehnt, hat es mich eher an ITIL v2 erinnert (was schliesslich auch COBIT mit beeinflusst hat). Viele Punkte bei den Tasks (und/oder best practices) sind doch recht operativ und könnten auch dem IT Management statt der IT Governance zugeordnet werden.*
- *Andererseits wird z.B. in DP01.T01 Best practices Compliance nebenbei erwähnt, was bei einer Implementierung einen erheblichen Aufwand bedeuten kann bis hin zu einem - je nach Fall - notwendigen Compliance Management.”* (Thiel, 2012)

3. Test review by Hugo Bosshard, Studerus AG

Hugo Bosshard works as head of IT at Studerus AG, a distributor of networking products and services. With more than 25 years of practical experience in this area, Hugo Bosshard is an exceptional candidate for reviewing and assessing the framework regarding its applicability.

For the test review, the following conditions were set:

- It should take no longer than half a day to understand the general purpose and the overall structure of the framework.
- The reviewer should be able to recognize first need of action during the completion of the assessment.
- The proper implementation of the framework within half a year should be reasonable.

These conditions were specified in order to be better able to prove the hypothesis. The study of larger frameworks like COBIT 5 (ISACA, 2012) usually requires significantly more time than just half a day and also the implementation usually takes longer than six months. These conditions are important factors that endorse the implementation of this tailored framework and especially in small and medium sized enterprises it is very important to keep the complexity of governance structure at a manageable level.

3.1 Test Review

"Das Assessment habe ich in der Zwischenzeit durchgeführt (Firmeneintrag mit Studerus AG). Das Studium des Frameworks innerhalb einer Woche sollte wirklich kein Problem darstellen. In meinem Falle habe ich einen halben Tag eingesetzt und beim Durchlesen auf unsere interne Situation referenziert. Zudem hat mir das Framework auch aufgezeigt, dass in einzelnen Bereichen Nachholbedarf besteht, d.h. hier konnte ich bereits einen Nutzen erkennen. Allerdings bin ich auch der Meinung, dass die Umsetzung in einer typischen KMU je nach Auslastung der IT-Verantwortlichen und vorherrschenden Ausgangslage 3 – 6 Monate beanspruchen kann. Sollte auch die Umsetzung eines IKS bevorstehen, könnten auch dort wertvolle Inputs gemacht werden." (Bosshard, Test Review, 2012)

4. Interpretation of Testimonials and Test Review

Compliance, outsourcing and the distinction between IT governance and IT management are the main issues that arose during the review and testing process. The compliance aspect does not seem to be satisfyingly covered by the framework. Compliance with external laws and regulations is difficult to manage. There may also be situations in whose companies are not aware that they have to be compliant with some regulations. A comprehensive implementation of the framework does not imply compliance with all relevant laws and regulations. However, the author tried to give concrete hints within the framework where compliance issues may come up.

Considering outsourcing, Service Level Management is not covered by the framework but several processes within the framework (especially in the domain Continuity) require proper management of also external suppliers. Although these processes do not completely cover the Service Level Management, the author believes to have found the right balance for small and medium-sized enterprises.

The result of the test review shows that the prescribed conditions could be fulfilled. The tester was able to understand the structure of the framework in a short time with no extensive studies of the framework. Also the provided assessment proves to be a good starting point. By filling out the assessment, the tester automatically becomes confronted with real life situations and the author believes that this linkage between daily business and governance topics is the foundation for a successful IT governance implementation. The estimation of the time that is needed to implement IT governance according to this framework is in line with the condition. The fulfillment of all of these conditions constitutes a major advantage compared to COBIT 5 or comparable frameworks.

Due to the missing basic population of test reviewers, this conclusion cannot be taken as a representative statement. A broad experiment would be necessary in order to gain a representative statement and the given time frame did not allow conducting such an experiment. However, the results of the interviews and the test review delivered important hints regarding the design of the framework.

Last but not least, according to both Thiel (Thiel, 2012) and Bitterli (Bitterli, Testimonial, 2012), the framework rather supports IT management than IT governance. From the author's point of view, this argument needs special consideration and is therefore discussed in the following chapter.

4.1 IT Governance versus IT Management

The conducted research revealed that one of the most significant characteristics in IT departments of small and medium-sized enterprises is that the demands that are posed against IT operations are high and sometimes even alike the aspirations that large enterprises have to their IT. Data and applications have to be available all the time, accessible from everywhere. Already small interruptions can have a severe impact to the business and therefore it is vital that IT processes are properly managed. Unlike the demand regarding the reliability of the IT department, the maturity level for most IT governance activities in small and medium-sized enterprises is drastically lower than in large enterprises. The following figure illustrates this imbalance which is here called the governance gap.

Important to notice is that this situation is not representative for all enterprises. Other factors like the industry sector have great influence to the size of the governance gap. However, during the research activities, this general pattern has proven to be right and was therefore taken into account at the early design phase of the framework.

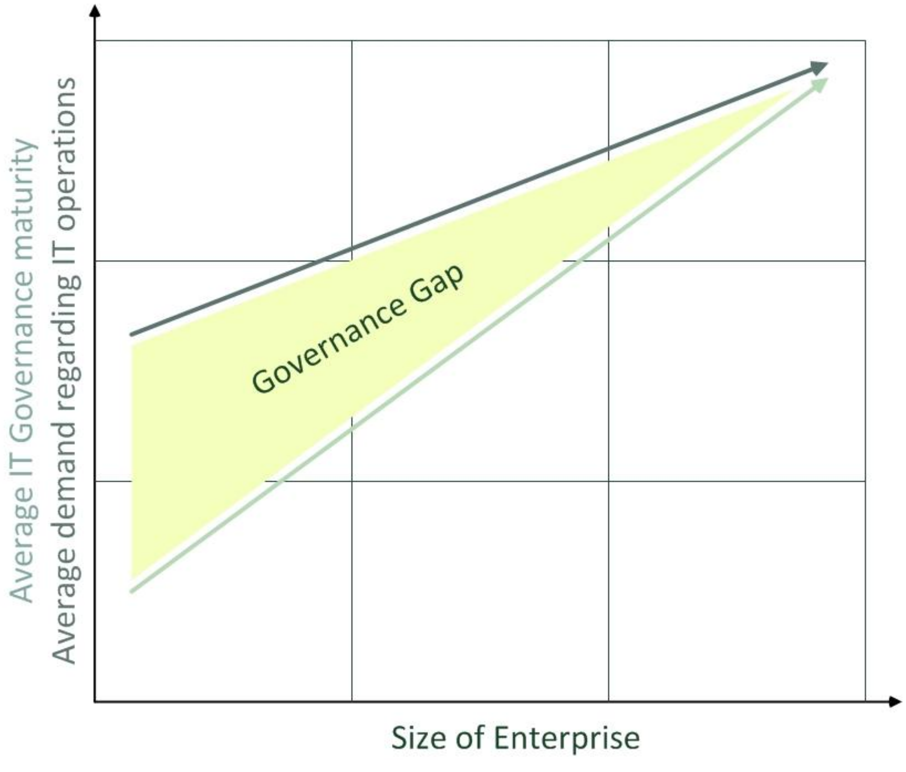


Figure 30: Governance gap.

In consequence of this circumstance, the demands of small and medium-sized enterprises towards IT governance are different than those of large companies. The top principle of any IT department should be to ensure stable and value-enabling IT operations at minimal cost, with the highest possible security measures. Due to the fact that IT departments face the same challenges independent of the quantity of their end-users, smaller enterprises have to put a stronger focus to operational issues because the necessary budget for proper IT governance activities is missing or the contribution to the value of such activities is not recognized. This condition could be observed during the interviews.

A bigger governance gap does not automatically mean that the IT department does not have the control over their processes. The existence of this imbalance between the required attention that is paid to either IT governance activities or operational issues only delivers reasonable justification for the broad orientation of the scope of the framework.

The implication for the design of the framework is that, unlike for example COBIT 5, the bulk of processes prescribed in the framework treat operational themes rather than pure governance topics. This strong orientation to operational issues accommodates to the demands that are posed to an IT governance framework for small and medium-sized enterprises. However rather operational issues are covered, the framework still remains a framework for IT governance and not IT management. Furthermore, the meanings of these terms tend to merge together when they are used in context with small and medium-sized enterprises.

To put it simply the framework that is presented in this paper aims to satisfy the needs of small and medium-sized enterprises concerning the governance of the most relevant IT processes that are typically present in enterprises of this target group.

5. Conclusion

Good governance of enterprise IT is in any case a benefit for all companies. Although the added value has not been quantifiably proven, previous research papers and also the results of the survey conducted in this paper clearly indicate that IT governance activities help to improve the IT alignment to the business. The assumption of the thesis is that there is a better way for small and medium-sized enterprises of governing enterprise IT than it is possible with the existing means. In the following, the hypothesis is repeated.

"IT governance in small and medium-sized enterprises leaks of proven implementation guidance and a suitable common agreed framework. A combination and tailoring of existing frameworks, which are mainly applicable for large organizations (including CobIT, ValIT, RiskIT, ISO27000, CMMI), will be a possible solution to provide a baseline IT governance approach for small and medium-sized enterprises."

According to the testimonials and the statement of applicability, the framework is an effective means to implement simple IT governance structures. The framework is easily understandable and does not need exhaustive resources for implementation. The author believes to have found the right balance between applicability and implementation effort and therefore considers that the hypothesis is corroborated. However, further testing must be made because of the missing basic population of examiners.

VII. Overall Conclusion

The significance of IT governance activities has emerged during the last couple of years. With the ongoing homogenization and standardization of IT products and services proper management and control of IT resources has become inevitable. The main goal of IT governance is to align the IT with the business requirements and processes and to maximize the value delivery of IT. To understand the term IT governance, an analysis of term IT governance is provided in this thesis. In the scientific literature, diverse definitions for IT governance have been published whereof the definition of Weill & Ross and the IT Governance Institute are considered to be the most significant ones. However, all the definitions have a certain catchphrase character in common which is a good indication and clears the way for a common agreed definition. The significance of a common agreed definition should not be underestimated. Though definitions are only descriptions of a term, they make a big contribution for a common understanding.

In this thesis, an IT governance framework for small and medium-sized enterprises is presented. The analysis of existing research has shown that IT governance has some positive impact for the overall business success; however it could not be proved from a qualitative perspective. The analysis has further shown that there are no adequate instruments that enable the implementation and operation of IT governance activities and this is the main trigger for this thesis.

The requirements from small and medium-sized enterprises regarding IT governance are significantly different from large companies. The presented survey and the interviews helped to find these requirements. The setup of the research activity was the right choice and the results delivered valuable input for the design of the framework. Whilst the interviews helped with the problem identification, the consolidated results of the survey delivered a quantitative basis for the structure of the framework. The result of the requirements analysis is that the framework is structured in a pyramid like depiction with the respective layers, domains and processes.

Another substantial input from the interviews is that small and medium-sized enterprises are, in terms of IT, organized much more individual. IT departments in large companies are mostly managed in a similar way, meaning that the organizational structure and procedures look pretty much the same in any enterprise. This statement does not hold true for small and medium-sized enterprises. The circumstance that IT departments in small and medium-sized enterprises are managed in many different ways and that almost nowhere standardized processes are in place is a major challenge for the design of the framework. Because of that, the framework must be applicable by any IT organization and this is the main reason why roles and responsibilities have not been prescribed in the framework.

The framework helps companies to improve their management of IT resources. This statement is confirmed by both, the testimonials of the industry experts and the statement of applicability of the testing enterprise. Of course, the framework cannot be considered to be the solution to all of the problems that IT departments face. Retrospectively, the review and testing phase is as important as the requirements analysis and the framework design. For time reasons, it was not possible to extend the testing activity (statement of applicability) and the author believes that further test implementations at potential end users would provide further valuable feedback for the improvement of the framework.

From the author's perspective, the enlisted principles are fulfilled by the framework. The framework is easily understandable and implementable and does not take as much effort for implementation as other frameworks. Especially for small and medium-sized enterprises it is vital to keep the maintenance effort of the framework on a minimum and thereby reducing the administrative overhead. Companies should not implement the framework for its own sake but should profit from the benefit of a well governed IT department. The fundamental orientation on the COBIT framework ensures both, validity and upwards compatibility. The upwards compatibility is a chance for the framework to be considered as the starting point towards IT governance.

The provided lifecycle eases the implementation and the assessment delivers an accurate view about the current situation. The assessment at the beginning of the IT governance initiative is a good opportunity for obtaining the management commitment. Additionally, it clearly depicts the discovered weaknesses, allocates them to the respective process in the framework and thereby supports the implementation team by prioritizing the planned measures.

Following the results of the expert reviews and the statement of applicability, the positive proof of the hypothesis is well on the way. It would be of greatest interest to see several practical implementations of the framework. Only with practical experience, the added value of using this framework emerges. The main challenge at this point will be to propagate the framework and to awake the interest of potential end-users. It is not the thing that small and medium-sized companies have been watching for an IT governance framework supporting them by improving their internal IT. It is even more the case that IT governance is considered to be a luxury topic and those only highly profitable companies can address it. Especially at small and medium-sized enterprises, the rethinking from the bottom-up to the top-down approach has not yet occurred. In many companies, IT still does not attract the attention that it deserves and the dependence on the IT processes is heavily underestimated. IT at small and medium-sized enterprises can be compared to our own health. We only appreciate the healthiness when we feel sick, and so does it happen with IT.

List of Literature

Bea, F. X., & Hass, J. (2005). *Strategisches Management.* Stuttgart: UTB-Verlag.

Bensch, A. (2006, 04 04). *IT-Governance in Versicherungsunternehmen.* Retrieved from http://www.uni-leipzig.de/~fvi/dokumente/lehrstuhl_vi/roof/IT-Governance_in_VU-Adrian_Bensch.pdf

Bitterli, P. R. (2006). *Praxishandbuch COBIT* (1. ed.). Symposium Publishing.

Bitterli, P. R. (2011, 03). IT-Governance - auch für KMU notwendig und sinnvoll. *ITMagazine, 2011/03*, 74-78.

Bitterli, P. R. (2012). *Testimonial.*

Bosshard, H. (2012, February 29). Interview Studerus AG.

Bosshard, H. (2012). *Test Review*.

Busta, B., Portz, C., Strong, J., & Lewis, R. (2006, July). Expert Consensus on the Top IT Controls. *ISACA Journal*.

Carr, N. (2003, May). IT Doesn't Matter. *Harvard Business Review*.

Committee on the Financial Aspects of Corporate Governance. (1992). Cadbury Report.

Cubeles-Marquez, A. (2008). IT Project Portfolio Management - The Strategic Vision of IT Projects. *Upgrade - The European Journal for the Informatics Professional, 1*(4), pp. 31 - 36.

De Haes, S., & van Grembergen, W. (2004). IT Governance and Its Mechanisms. *Information Systems Control Journal*(1).

Europäische Kommission. (2006). *Die neue KMU-Definition. Benutzerhandbuch und Mustererklärung.*

Fachstab für Informatik der Treuhand Kammer. (2010). *Vorgehensmodell IT-Risikoanalyse - Arbeisthilfe für KMU Prüfer.* Treuhand Kammer.

Grünendahl, R. T., Steinbacher, A. F., & Will, P. H. (2012). *Das IT-Gesetz: Compliance in der IT-Sicherheit* (2. ed.). Wiedbaden: Springer Verlag.

Hamer, E. (2006). *Betriebswirtschaftslehre der Mittel- und Kleinbetriebe. Größenspezifische Probleme und Möglichkeiten zu ihrer Lösung.* Berlin: Erich Schmidt Verlag.

Heinrich, L. J., & Lehner, F. (2005). *Informationsmanagement - Planung, Überwachung und Steuerung der Informationsinfrastruktur.* München: Oldenburg-Verlag.

Henderson, J. C., & Venkatraman, N. (1989). Strategic Alignment: A Framework for Strategic Information Technology Management. (C. f. Research, Ed.)

Holtschke, B., Heier, H., & Hummel, T. (2009). *Quo vadis CIO.* Heidelberg: Springer-Verlag.

International Organization for Standardization. (2008). *ISO/IEC 38500.* International Organization for Standardization.

ISACA. (2007). *CobIT 4.1.* (ISACA, Ed.) ISACA.

ISACA. (2008). *The Val IT Framework 2.0.* ISACA.

ISACA. (2012). *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT.* Rolling Meadows, USA.

ISACA. (2012). *COBIT 5 - Enabling Processes.* Rolling Meadows, USA.

ISACA. (2012). *COBIT 5 - Executive Summary.* ISACA.

IT Governance Institute & KPMG. (2003). *IT Governance für Geschäftsführer und Vorstände* (zweite Ausgabe ed.). IT Governance Institute and KPMG.

IT Governance Institute. (2003). *Board Briefing on IT Governance, 2nd Edition.*

IT Governance Institute. (2008). *IT Governance Global Status Report 2008.*

IT Governance Institute. (2009). IT Governance Roundtable: Defining IT Governance.

Johannsen, W., & Goeken, M. (2011). *Referenzmodelle für IT-Governance.* Heidelberg: dpunkt.verlag.

Kaplan, R. S., & Norton, D. P. (1992, January). The Balanced Scorecard - Measures that Drive Performance. *Harvard Business Review*, pp. 71 - 79.

Kopp, C. (2009). *Vorgehensmodell für die Einführung von IT-Governance in mittelständischen Unternehmen - Vorgehensmodell für die Einführung mit den Referenzmodellen COBIT, ITIL und Val-IT.* Master's thesis, Hochschule Liechtenstein - Fachbereich Wirtschaftsinformatik.

Kremar, H. (2004). *Informationsmanagement.* Heidelberg: Springer-Verlag.

Kunz, H. (2011). *IT Governance for small and medium enterprises.* Master's thesis, University of Applied Sciences Northwestern Switzerland - School of Business.

Landolt, C. (2009). *Lohnt sich IT-Governance auch für KMU - Eine empirische Untersuchung schweizerischer Industrieunternehmen.* Master's thesis, Universität Zürich - Institut für Informatik.

Leitner, K. (2001). Strategisches Verhalten von kleinen und mittleren Unternehmen. Eine empirische Untersuchung an österreichischen Industrieunternehmen vor einem indsutrieökonomischen Hintergrund. Wien: Fakultät für Wirtschaftswissenschaften und Informatik der Universität Wien.

Lindstöm, A., Gammelgard, M., Simonsson, M., & Jonsson, N. (2005). *A method to assess the enterprise-wide IT resources for performance and investment justifications.* New Jersey, USA: Proceedings of the Conference on Systems Engineering Research (CSER).

Macdonald, H. K. (1994). Organisational Transformation and Alignment: Misalignment as an Impediment to Progress in Organisational Development. *Information Management & Computer Security, 4*(2), pp. 16 - 19.

Martin, J. R. (2012, 01 18). *Balanced Scorecard Summary*. Retrieved from maaw.info: http://maaw.info/images/BalancedScorecardFramework.gif

Organisation for Economic Co-operation and Development. (2004). *OECD Principles of Corporate Governance.* Paris.

Pfeifer, A. (2003). *Zum Wertbeitrag von Informationstechnologie. Eine Darstellung an Unternehmen der Fertigungsbrnachen in Deutschland.* Passau, Germany.

Pfohl, H.-C. (2006). *Unternehmensführung. In Betriebswirtschaftslehre der Mittel- und Kleinbetriebe.Grössenspezifische Probleme und Möglichkeiten zu ihrer Lösung.* Berlin: Erich Schmidt Verlag,.

Project Management Institute. (2009). *A Guide To The Project Management Body Of Knowledge (PMBoK Guide)* (4 ed.). Project Management Institute.

Rüter, A., Schröder, J., & Göldner, A. (2006). *IT-Governance in der Praxis.* Berlin, Germany: Springer-Verlag.

Saunders, M., Lewis, P., & Thornhill, A. (2004). *Research Methods for Business Students.* Prentice Hall.

Schweizerische Eidgenossenschaft. (2005). *Hermes - Führen und Abwickeln von Projekten der Informations- und Kommunikationstechnik (IKT).* Bern.

Thiel, C. (2012). *Testimonial.*

Weill, P. (2004). *Don't Just Lead, Govern: How Top-Performing Firms Govern IT.* MITSloan Center for Information Research.

Weill, P., & Ross, J. W. (2004). *IT Governance - How Top Performers Manage IT Decision Rights for Superior Results.* Harvard Business.

Zurbrügg, M. (2012, February 15). Interview Informaticon AG.

Glossary of Terms

BSC	Balanced Scorecard
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CGEIT	Certified in the Governance of Enterprise IT
COBIT	Control Objectives for Information and Related Technology
CRM	Customer Relationship Management
ERP	Enterprise Resource Planning
IKS	Internes Kontrollsystem
IT	Information Technology
ITGI	IT Governance Institute
ITIL	IT Infrastructure Library
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
MIT	Massachusetts Institute of Technology
OECD	Organisation for Economic Co-operation and Development
PMBoK	Project Management Body of Knowledge
RACI	A responsibility alignment matrix
ROI	Return on Investment
SAM	Strategic Alignment Model
SLA	Service Level Agreement
UTM	Unified Threat Management
USB	Universal Serial Bus
VPN	Virtual Private Network

List of Figures

List of Tables

Appendix

Appendix A – Consolidated Survey Results

Due to privacy reasons, the survey results have been anonymized.

Company A - Survey Results

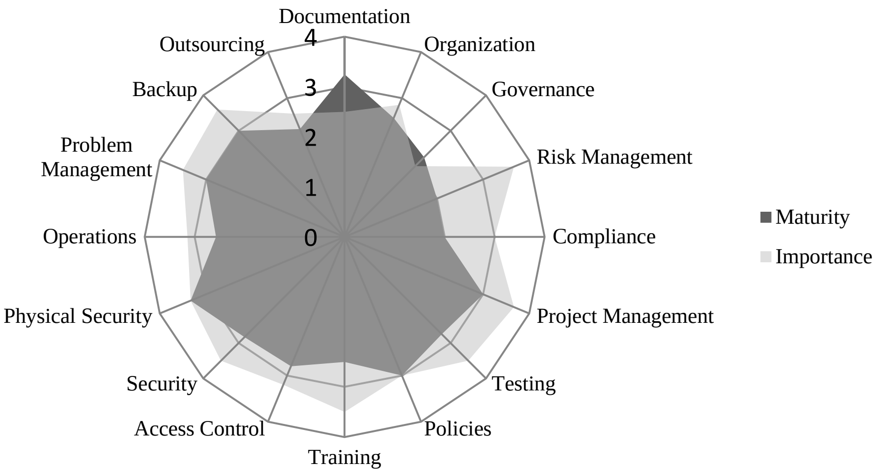


Figure 31: Survey results - Company A.

Company B - Survey Results

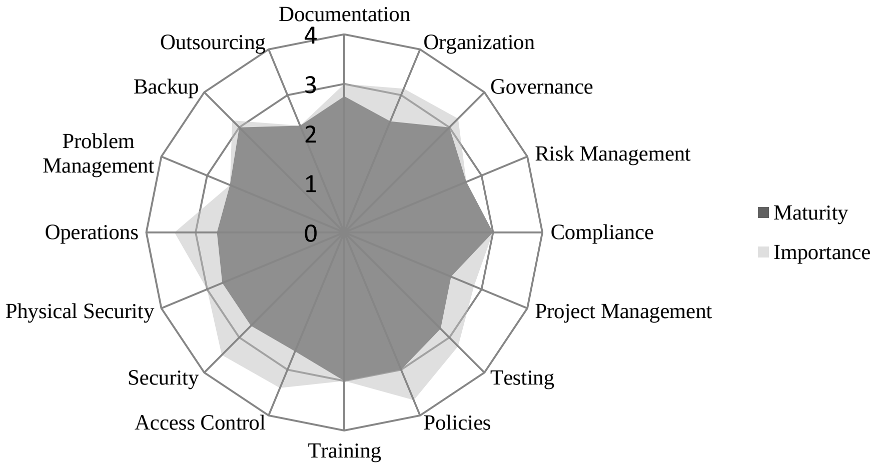


Figure 32: Survey results - Company B.

Company C - Survey Results

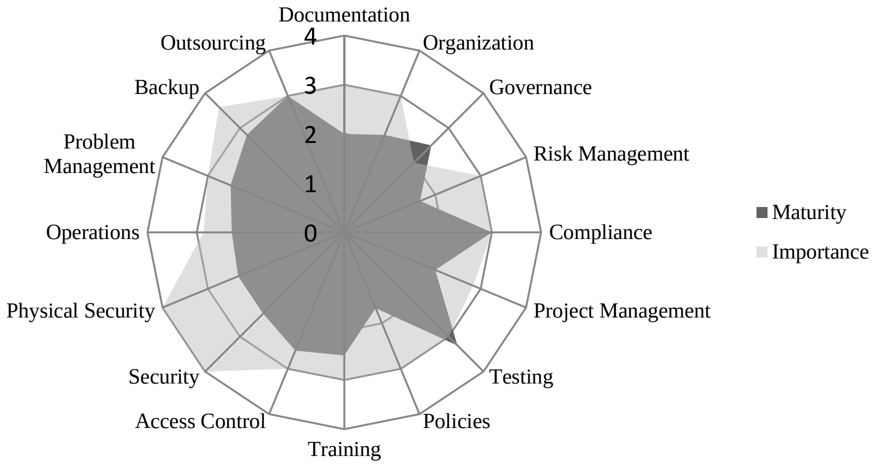


Figure 33: Survey results - Company C.

Company D - Survey Results

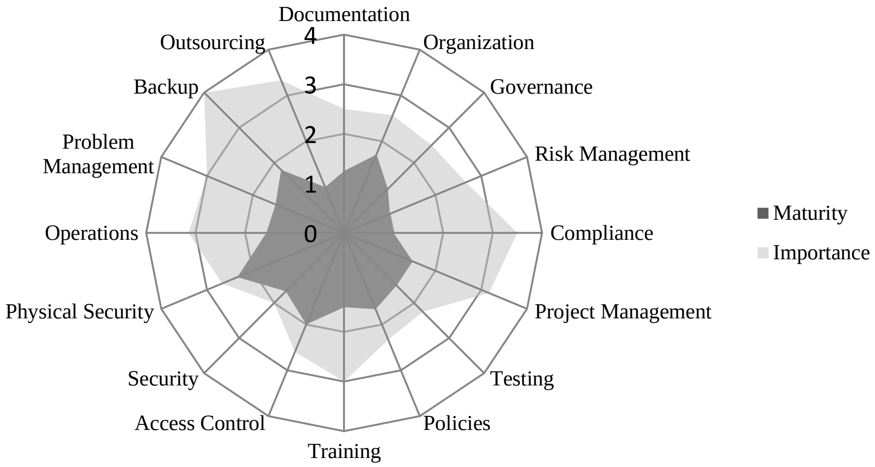


Figure 34: Survey results - Company D.

Company E - Survey Results

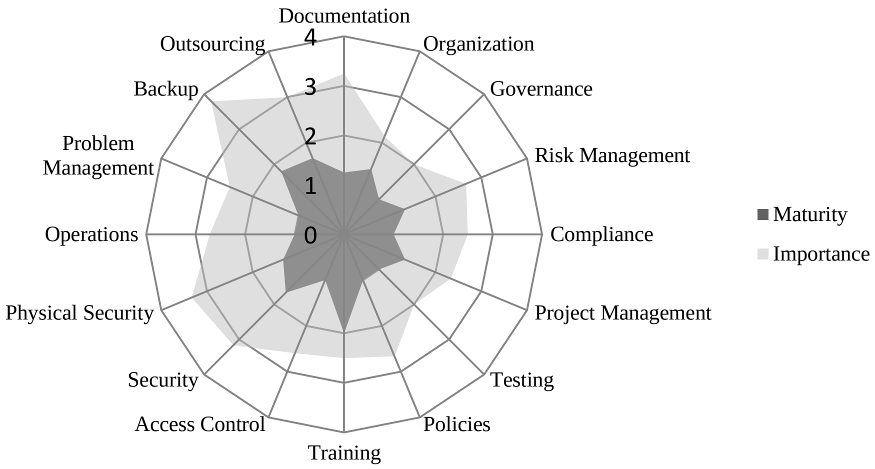


Figure 35: Survey results - Company E.

Company F - Survey Results

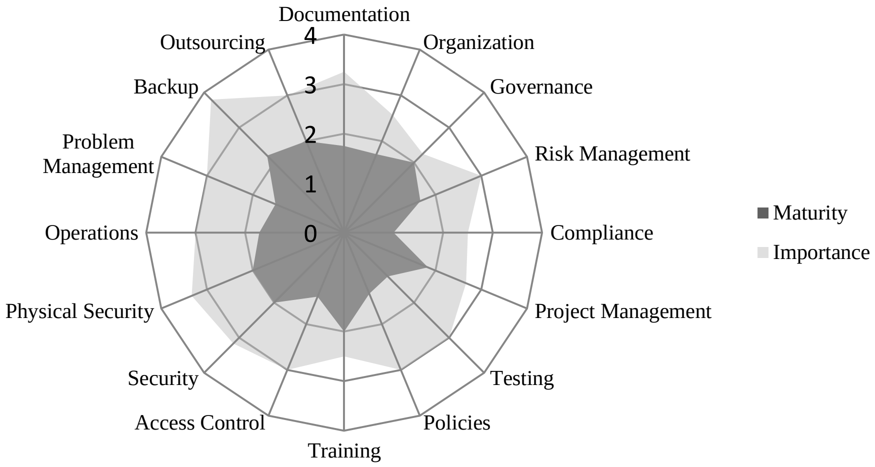


Figure 36: Survey results - Company F.

Company G - Survey Results

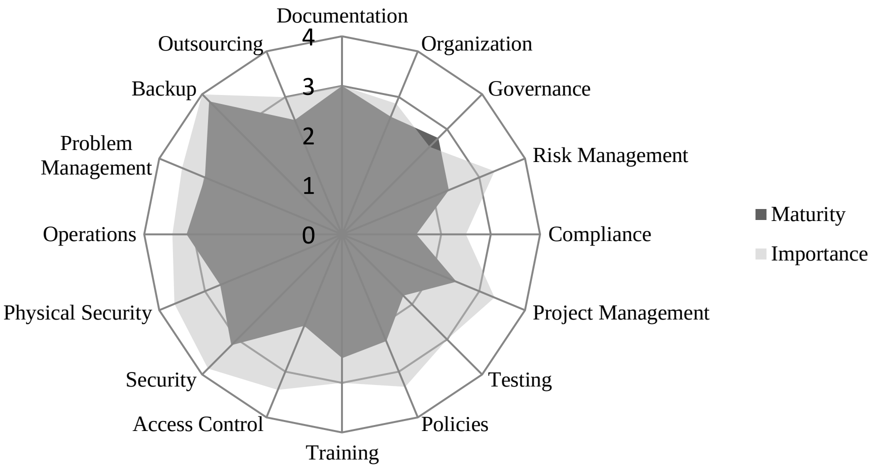


Figure 37: Survey results - Company G.

Appendix B – Detailed Survey Results

Appendix B contains the detailed Survey Results. The questions are out of the Vorgehensmodell IT-Risikoanalyse – Arbeitshilfe für KMU (Fachstab für Informatik der Treuhand Kammer, 2010). On the left half of the Table, the answers of the companies (A-G) are depicted. (M = Maturity / I = Importance)

Detailed Results – Documentation

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	Maturitätsstufe 2	Maturitätsstufe 3	Maturitätsstufe 4	M	I	M	I	M	I	M	I	M	I	M	I	M	I	M	I
Übersicht IT-Infrastruktur	Es besteht keine Übersicht über die Informatik-Infrastruktur.	Es besteht eine veraltete (älter als 1 Jahr) Übersicht über die Informatik-Infrastruktur.	Eine aktuelle Übersicht der wesentlichen Komponenten der Informatik-Infrastruktur (Systeme und Vernetzung) besteht. Beschaffungs-, Projekt- und Änderungsprozesse führen nicht zwangsläufig zu einer Aktualisierung dieser Übersicht.	Eine aktuelle Übersicht der gesamten Informatik-Infrastruktur (Systeme und Vernetzung) besteht. Beschaffungs-, Projekt- und Änderungsprozesse beinhalten die zwingende Aktualisierung dieser Übersicht.	3	4	2	3	2	3	2	3	1	4	2	3	3	3	2.14	2.71
Hadrware-Inventare	Es besteht kein Hardware-Inventar.	Es besteht ein veraltetes (älter als 1 Jahr) Hardware-Inventar.	Ein Hardware-Inventar wird aktuell geführt; Beschaffungsprozesse stellen jedoch die zwingende Aktualisierung dieses Inventars nicht sicher.	Ein Hardware-Inventar wird aktuell und vollständig geführt. Beschaffungs- und Projektprozesse beinhalten die zwingende Aktualisierung dieses Inventars sowie Anpassung/Abschluss allfälliger Wartungsverträge.	3	2	3	3	1	3	1	3	1	3	1	4	3	3	1.86	2.29
Software-Inventare	Es besteht kein Software-Inventar.	Es besteht ein veraltetes (älter als 1 Jahr) Software-Inventar.	Ein Software-Inventar (auch für die Lizenzkontrolle) wird aktuell geführt; Beschaffungsprozesse stellen jedoch die zwingende Aktualisierung dieses Inventars nicht sicher.	Ein Software-Inventar (auch für die Lizenzkontrolle) wird aktuell und vollständig geführt. Beschaffungs- und Projektprozesse beinhalten die zwingende Aktualisierung dieses Inventars sowie die Klärung allfälliger Lizenzierungs- und Nachlizenzierungsfragen.	3	2	3	3	3	3	1	3	1	3	2	3	3	3	2.29	2.43
Verträge und Dienstleistungsvereinbarungen	Es bestehen kaum Verträge zwischen dem Informatikbereich und Dritten, obwohl Leistungen bezogen werden.	Es bestehen eine Übersicht/ Zusammenstellung von im Informatikbereich relevanten Verträge mit Dritten (Lieferanten, Kunden, Partner); diese ist jedoch unvollständig und nicht aktuell.	Es besteht eine Übersicht/ Zusammenstellung aller im Informatikbereich relevanten Verträge mit Dritten (Lieferanten, Kunden, Partner).	Es besteht eine Übersicht/ Zusammenstellung aller im Informatikbereich relevanten Verträge mit Dritten (Lieferanten, Kunden, Partner). Sie wird zentral und aktuell geführt und beinhaltet alle Verträge sowie zugehörigen Dokumente wie SLA usw.	4	2	3	3	2	3	1	1	2	3	2	3	3	3	2.43	2.29
Durchschnitt																			2.18	2.43

Detailed Results – Organization

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Verantwortlichkeiten	Die Verantwortlichkeiten für Einführung, Betrieb, Unterhalt und Schutz von IT-Ressourcen sind nicht geregelt.	Die Verantwortlichkeiten für Einführung, Betrieb, Unterhalt und Schutz von IT-Ressourcen werden in der Regel informell übertragen.	Die meisten Verantwortlichkeiten für Einführung, Betrieb, Unterhalt und Schutz von IT-Ressourcen sind schriftlich dokumentiert. Die Dokumentation wird jedoch nicht zentral verwaltet und ist teilweise veraltet.	Die Verantwortlichkeiten für Einführung, Betrieb, Unterhalt und Schutz von IT-Ressourcen sind in Stellenoder Prozessbeschreibungen schriftlich dokumentiert. Diese Dokumentationen werden bei Bedarf – aber mindestens jährlich – überprüft und angepasst.	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**2**	**2**	**3**	**2**	**2**	**3**	**3**	**2.71**	**2.71**
Architektur / Technologie	Neue Technologien werden umgehend eingeführt, ohne dass ihr wirtschaftlicher oder strategischer Nutzen und ihr korrektes Funktionieren in der bestehenden Umgebung nachgewiesen ist.	Neue Technologien werden umgehend eingeführt, wenn sie einen wirtschaftlichen oder strategischen Vorteil versprechen. Vor dem ersten Einsatz werden teilweise technische Abklärungen durchgeführt.	Neue Technologien werden erst eingeführt, wenn sie sich am Markt etabliert haben und Referenzen verfügbar sind. Vor dem ersten Einsatz werden die üblichen Tests durchgeführt.	Neue Technologien werden systematisch evaluiert und auf ihre Bedeutung für die IT-Strategie geprüft. Vor dem ersten Einsatz werden neue Produkte auf Funktionalität, Zuverlässigkeit und Kompatibilität ausserhalb der produktiven Umgebung umfassend getestet.	**4**	**4**	**3**	**4**	**2**	**4**	**3**	**2**	**3**	**2**	**3**	**4**	**4**	**3**	**3.14**	**3.29**
Funktionentrennung	Es besteht innerhalb der IT keine Funktionentrennung; kritische Funktionen (z.B. Entwickler/Operator) werden nicht getrennt.	Es besteht innerhalb der IT nur eine rudimentäre, informelle Funktionentrennung; kritische Funktionen (z.B. Entwickler/Operator) werden nicht getrennt.	Es besteht eine Funktionentrennung für kritische IT-Funktionen; diese ist aber nicht dokumentiert und wird nicht weiter überwacht.	Es wird innerhalb des ITFachbereichs konsequent auf eine funktionale Funktionentrennung geachtet; diese ist in den Aufgabenbeschreibungen dokumentiert und deren Einhaltung wird ständig überwacht.	**2**	**1**	**2**	**3**	**2**	**3**	**1**	**3**	**1**	**1**	**2**	**2**	**3**	**2**	**1.86**	**2.14**
Stellvertretung	Es besteht innerhalb der IT keine Stellvertretungsregelung.	Es besteht innerhalb der IT nur eine rudimentäre Stellvertretungsregelung.	Für die wichtigsten Positionen innerhalb der IT sind Stellvertretungen definiert aber kaum geschult; entsprechende Dokumentationen sind teilweise vorhanden und unterstützen die Durchführung der Tätigkeiten durch den/die Stellvertreter.	Für alle wesentlichen Positionen innerhalb der IT sind Stellvertretungen vorhanden und geschult; entsprechende aktuelle Dokumentationen ermöglichen de facto die Durchführung der Tätigkeiten durch den/die Stellvertreter.	**3**	**4**	**2**	**4**	**2**	**3**	**2**	**3**	**1**	**3**	**2**	**3**	**3**	**4**	**2.14**	**3.43**

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	Maturitätsstufe 2	Maturitätsstufe 3	Maturitätsstufe 4	M	I	M	I	M	I	M	I	M	I	M	I	M	I	M	I
Freigabeverfahren für IT-Infrastrukturänderungen	Es existieren keine Freigabeverfahren für Änderungen im IT-Infrastrukturbereich.	Es existieren informelle Freigabeverfahren für Änderungen im IT-Infrastrukturbereich.	Für sämtliche IT-Infrastrukturbereiche sind formelle Freigabeverfahren für Änderungen definiert, diese können jedoch umgangen oder ausgelassen werden.	Für sämtliche IT-Infrastrukturbereiche sind formelle Freigabeverfahren für Änderungen definiert. Ihre Einhaltung wird durchgesetzt und regelmässig überprüft. Änderungsanträge ohne die notwendigen Freigaben werden konsequent zurückgewiesen.	2	3	3	3	2	3	1	3	1	3	1	3	2	3	1.71	3.00
Nachvollziehbarkeit von Freigaben für IT-Infrastrukturänderungen	Freigaben für Änderungen an der IT-Infrastruktur werden nicht schriftlich festgehalten.Freigaben für Änderungen an der IT-Infrastruktur werden nicht schriftlich festgehalten.	Es existieren kaum Aufzeichnungen von Freigaben für Änderungen an der IT-Infrastruktur.	Die meisten Freigabevorgänge für Änderungen an der IT-Infrastruktur sowie die Änderungen selbst werden aufgezeichnet; eine Überwachung findet hingegen nur punktuell statt.	Alle Freigabevorgänge für Änderungen an der IT-Infrastruktur sowie die Änderungen selbst werden lückenlos aufgezeichnet. Die Einhaltung der Freigabeprozesse wird laufend überwacht und regelmässig kontrolliert.	1	2	2	2	2	3	1	3	1	2	1	2	2	3	1.43	2.43
Kostenkontrolle	IT-Kosten werden in der Buchhaltung nicht nach klaren Vorgaben einheitlich behandelt. Die Zurechnung von Kosten und Zeiten zu IT-Aktivitäten ist nicht möglich.	Kosten für die IT werden budgetiert und laufend erfasst. Eine Aufschlüsselung zu einzelnen IT-Aktivitäten findet jedoch nicht statt. Bei Projekten erfolgt keine Nachkalkulation.	Kosten für die IT werden global budgetiert und laufend erfasst. Eine Aufschlüsselung zu einzelnen IT-Aktivitäten findet jedoch nicht statt. Bei grösseren Projekten erfolgt eine Nachkalkulation, wobei wesentliche Überschreitungen begründet werden.	Es gibt einen umfassenden Prozess zur finanziellen Kontrolle aller IT-Aktivitäten und IT-Projekte inkl. Planung, Budgetierung, Kosten- und Zeiterfassung und Ergebniskontrolle. Abweichungen werden systematisch analysiert.	3	3	2	3	2	2	1	2	1	1	1	2	1	2	1.57	2.14
Durchschnitt																			2.08	2.73

Detailed Results – Governance

Kriterium	**Description of Maturity**				**A**		**B**		**C**		**D**		**E**		**F**		**G**		**Durchschnitt**	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Abgestimmte IT-Infrastruktur	Beschaffung, Betrieb und Wartung der IT-Infrastruktur folgen einer vom Business unabhängigen Strategie.	Beschaffung, Betrieb und Wartung der IT-Infrastruktur folgen keiner übergeordneten, aus den Geschäftszielen abgeleiteten Strategie. Orientiert sich im Ansatz aber am Business.	Das Unternehmen achtet darauf, dass die IT-Infrastruktur abgestimmt auf die Geschäftsziele beschafft, betrieben und gewartet wird; es existiert hierzu jedoch kein formalisierter Prozess.	Es besteht ein formalisierter Prozess, der sicherstellt, dass IT-Infrastruktur abgestimmt auf die Geschäftsziele beschafft, betrieben und gewartet wird.	**1**	**1**	**3**	**3**	**3**	**3**	**2**	**3**	**1**	**3**	**2**	**3**	**3**	**3**	**2.14**	**2.71**
Vorgaben für IT (SLA)	Zwischen der IT-Abteilung und den Fachabteilungen (Benutzern) bestehen keinerlei Leistungsvereinbarungen bezüglich Servicezeiten, Verfügbarkeit und Performance der IT-Dienstleistungen.	In der IT-Abteilung bestehen Leistungsziele für die Erbringung ihrer Services. Diese sind nicht kommuniziert oder mit den Fachabteilungen abgesprochen.	Zwischen der IT-Abteilung und den Fachabteilungen (Benutzer) bestehen informelle Leistungsvereinbarungen bezüglich Servicezeiten, Verfügbarkeit und Performance der IT-Dienstleistungen; diese sind jedoch nicht vollständig dokumentiert und werden nicht periodisch auf ihre Einhaltung geprüft.	Zwischen der IT-Abteilung und den Fachabteilungen (Benutzern) bestehen formelle Leistungsvereinbarungen bezüglich Servicezeiten, Verfügbarkeit und Performance der IT-Dienstleistungen in Form von schriftlichen SLA . Diese werden periodisch auf ihre Einhaltung geprüft.	**2**	**3**	**3**	**3**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**2**	**3**	**2**	**1.86**	**1.86**
IT-Governance	Es findet keine Steuerung der Informatik-Organisation und IT-Prozessen statt.	Die Gestaltung und Steuerung von Informatik-Organisation und -Prozessen orientieren sich an keinerlei Standards, sondern sind Eigenentwicklungen.	Die Gestaltung und Steuerung von Informatik-Organisation und IT-Prozessen orientieren sich an Standards wie CobiT (Governance), ITIL (Service-Management) sowie ISO 2700x (Sicherheits-Management).	Die Gestaltung und Steuerung von Informatik-Organisation und IT-Prozessen werden gemäss Standards wie CobiT (Governance), ITIL (Service-Management) sowie ISO 2700x (Sicherheits-Management) konsequent umgesetzt.	**3**	**2**	**3**	**3**	**3**	**2**	**1**	**3**	**1**	**2**	**2**	**2**	**2**	**2**	**2.14**	**2.29**
Dokumentation der IT-Prozesse	IT-Prozesse und zuständige Verantwortlichkeiten werden nicht kommuniziert. Einzelpersonen sind frei in ihrer Tätigkeit. Es findet keinerlei Überwachung und Kontrolle statt.	Die IT-Prozesse und zuständigen Verantwortlichkeiten werden informell kommuniziert und Einzelpersonen sind weitgehend frei in ihrer Tätigkeit. Es findet keinerlei Überwachung und Kontrolle statt.	Nur die wichtigsten ITProzesse und zuständigen Verantwortlichkeiten sind schriftlich festgehalten; diese Dokumentation ist nicht zwingend aktuell und korrekt. Die Einhaltung dieser Prozesse wird nur sporadisch überwacht; Kontrollen finden nur nach aussergewöhnlichen Ereignissen statt.	Alle relevanten IT-Prozesse und zuständigen Verantwortlichkeiten sind schriftlich, aktuell und den Tatsachen entsprechend dokumentiert; ihre Einhaltung wird laufend überwacht und regelmässig kontrolliert.	**3**	**2**	**3**	**4**	**3**	**2**	**1**	**3**	**1**	**2**	**2**	**2**	**3**	**3**	**2.29**	**2.57**
Durchschnitt																			**2.11**	**2.36**

Detailed Results – Risk Management

Kriterium	**Description of Maturity**				**A**		**B**		**C**		**D**		**E**		**F**		**G**		**Durchschnitt**	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Risikomanagement	IT-Risiken und Sicherheitserfordernisse werden nicht erhoben oder geprüft.	IT-Risiken und Sicherheitserfordernisse werden nur nach sicherheitsrelevanten Ereignissen geprüft. Die Umsetzung von geplanten Verbesserungsmassnahmen wird nicht überwacht.	IT-Risiken und Sicherheitserfordernisse werden in unregelmässigen Abständen oder wenig systematisch hinterfragt. Geplante Verbesserungsmassnahmen werden nur teilweise überwacht.	IT-Risiken und Sicherheitserfordernisse werden periodisch und systematisch hinterfragt und durch ein regelmässiges Control Self Assessment aktiv bearbeitet. Die vollständige Umsetzung geplanter Verbesserungsmassnahmen wird zeitnah überwacht.	**2**	**4**	**3**	**3**	**3**	**3**	**1**	**3**	**1**	**3**	**2**	**3**	**3**	**4**	**2.14**	**3.29**
Sicherheitspolitik	IT-Sicherheitspolitik und Sicherheitskonzept sind nur rudimentär vorhanden oder fehlen vollständig.	IT-Sicherheitspolitik und Sicherheitskonzept sind teilweise vorhanden, aber bereits älter als 1 Jahr.	IT-Sicherheitspolitik und Sicherheitskonzept werden in unregelmässigen Abständen überprüft und angepasst.	IT-Sicherheitspolitik und Sicherheitskonzept werden periodisch überprüft und an die konkrete Bedrohungslage sowie die aktuelle(n) Geschäftsstrategie/Geschäftsziele angepasst.	**2**	**4**	**3**	**3**	**1**	**3**	**1**	**2**	**1**	**3**	**1**	**3**	**2**	**3**	**1.57**	**3.00**
Versicherungen	Es bestehen keine Versicherungen für IT-Infrastrukturen und -Geräte (Hardware).	Für IT-Infrastrukturen und -Geräte (Hardware) bestehen teilweise Versicherungen; jedoch ist unklar, ob für alle möglichen Ereignisse eine angemessene Versicherungsdeckung besteht.	Für IT-Infrastrukturen und -Geräte (Hardware) besteht eine Sachversicherung; der Bedarf nach weiteren Versicherungen (z.B. Datenträger/ Mehrkosten, Betriebsunterbruch) ist informell geklärt.	Für IT-Infrastrukturen und -Geräte (Hardware) besteht eine Sachversicherung; der Bedarf nach weiteren Versicherungen (z.B. Datenträger/ Mehrkosten, Betriebsunterbruch) ist formell geklärt. Beschaffungs- und Projektprozesse beinhalten die zwingende Klärung zusätzlicher Versicherungsdeckung; es besteht eine zentrale aktuelle Übersicht aller abgeschlossenen Versicherungsleistungen.	**2**	**3**	**2**	**2**	**1**	**3**	**1**	**3**	**2**	**2**	**2**	**3**	**2**	**3**	**1.71**	**2.71**
Durchschnitt																			**1.81**	**3.00**

Detailed Results – Compliance

Kriterium	**Description of Maturity**				**A**		**B**		**C**		**D**		**E**		**F**		**G**		**Durchschnitt**	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Nichteinhaltung von Gesetzen / Normen / Vorschriften	Die Erkennung der Anwendbarkeit von Gesetzen, Normen und Vorschriften und der Einhaltung ist nicht geregelt.	Es gibt keine Vorkehrungen zur systematischen Erfassung von für das Unternehmen relevanten Gesetzen, Normen und Vorschriften und deren Einhaltung.	Die wichtigsten relevanten Gesetze, Normen und Vorschriften sind in den verschiedenen Fachabteilungen bekannt. Die Einhaltung wird bereichsweise geregelt.	Es existiert ein definierter Prozess zur Erfassung sämtlicher relevanten Gesetze, Normen und Vorschriften sowie klare interne Kontrollen zu ihrer Einhaltung.	**3**	**3**	**3**	**3**	**3**	**3**	**1**	**3**	**1**	**3**	**1**	**3**	**2**	**3**	**2.00**	**3.00**
Unabhängige Prüfung der IT	Es werden keine unabhängigen Prüfungen der IT-Anwendungen, der IT-Infrastruktur und des ITBetriebes durchgeführt.	Es werden kaum unabhängige Prüfungen der IT-Anwendungen, der IT-Infrastruktur und des IT-Betriebes durchgeführt. Massnahmen zur Behebung von erkannten Schwachstellen oder Lücken werden nicht umgesetzt.	Es werden zwar unabhängige Prüfungen der IT-Anwendungen, der IT-Infrastruktur und des IT-Betriebes durchgeführt, aber nur aufgrund spezifischer Ereignisse oder Anforderungen. Massnahmen zur Behebung von Schwachstellen oder Lücken werden nicht konsequent umgesetzt.	Es werden regelmässig unabhängige Prüfungen der IT-Anwendungen, der IT-Infrastruktur und des IT-Betriebes durchgeführt. Angemessene Massnahmen werden konsequent und zeitnah umgesetzt, die dazu notwendigen Arbeiten werden kontrolliert.	**1**	**3**	**3**	**3**	**3**	**3**	**1**	**4**	**1**	**2**	**1**	**2**	**1**	**2**	**1.57**	**2.71**
Durchschnitt																			**1.79**	**2.86**

Detailed Results – Project Management

Kriterium	**Description of Maturity**				**A**		**B**		**C**		**D**		**E**		**F**		**G**		**Durchschnitt**	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
IT-Projektmanagement (Portfolio)	Es besteht keine Übersicht über die informatikrelevanten Projekte.	Eine teilweise Übersicht über laufende IT-Projekte besteht; es gibt jedoch keine weiterführende Dokumentationen.	Eine aktuelle Übersicht aller informatikrelevanten Projekte besteht; es besteht jedoch keine zwingende Abstimmung mit einem unternehmensweiten Portfolio sämtlicher Projekte.	Es wird ein unternehmensweites Projekt-Portfolio gepflegt, dass auch alle informatikrelevanten Projekte einschliesst. Der Projektprozess beinhaltet die zwingende Abstimmung mit diesem Portfolie und dessen Aktualisierung.	**3**	**4**	**2**	**3**	**2**	**2**	**1**	**3**	**1**	**2**	**2**	**3**	**3**	**4**	**2.00**	**3.00**
Projektaufteilung in Phasen	Projekte werden kaum in Phasen unterteilt; Lieferobjekte oder Meilensteine fehlen zum grössten Teil.	Projekte werden in lange Einzelphasen ohne klare Lieferobjekte und Meilensteine unterteilt.	Projekte werden in wenige Phasen mit Lieferobjekten unterteilt; die frühen Planungsphasen (Pflichtenheft / Spezifikationen) werden typischerweise zugunsten der Durchführungsphase verkürzt. Eine Projektfortschrittskontrolle findet nur teilweise statt.	Projekte werden eindeutig in Meilensteine sowie verschiedene Haupt- und Unteraktivitäten mit klaren Lieferobjekten unterteilt (z.B. Pflichtenheft / Spezifikationen / Durchführung / Test / Abnahme / Einsatz); es finden regelmässige Sitzungen zum Projektfortschritt statt.	**3**	**2**	**3**	**2**	**3**	**3**	**2**	**4**	**1**	**2**	**1**	**2**	**2**	**3**	**2.14**	**2.57**
Projektteam	Es werden keine Teams benannt, Mitarbeiter werden dynamisch und unkoordiniert eingebunden.	Projektleiter und Teams werden informell benannt; es gibt aber keine klaren Aufgabenbeschreibungen. Eine Schulung der Projektteams in der angewandten Projektmanagementmethode hat kaum stattgefunden.	Es werden zwar Projektleiter und Projektteams benannt, doch deren konkrete Aufgaben wie auch der damit verbundene Zeitaufwand wurde nicht konsequent eingeplant. Eine Schulung der angewandten Projektmanagementmethode hat nur teilweise stattgefunden.	Es werden Projektleiter und Projektteams benannt und es wird klar festgelegt, wer für welche Aufgaben mit wie viel Prozent seiner Arbeitszeit im Projekt engangiert. Projektleiter wie sämtliche Projektmitarbeiter sind in der angewandten Projektmanagementmethode ausreichend geschult.	**2**	**4**	**2**	**2**	**2**	**3**	**1**	**4**	**1**	**1**	**1**	**2**	**2**	**2**	**1.57**	**2.57**
Grad der Mitwirkung der Geschäftsleitung in Projekten	Die Geschäftsleitung nimmt ihre Entscheidungsgewalt nicht wahr und hat diese auch nicht formell an einen Steuerungsausschuss oder an den IT-Verantwortlichen delegiert.	Die Geschäftsleitung (GL) delegiert ihre Entscheidungsgewalt z.B. an einen Steuerungsausschuss oder den IT-Verantwortlichen. Die Geschäftsleitung wird in Projekten nur auf Anfrage von Benutzervertretern oder IT-Verantwortlichen tätig.	Die Geschäftsleitung (GL) wird durch regelmässige Protokolle über den Projektfortschritt informiert; sie nimmt jedoch kaum an Projekt(steurungs)sitzungen oder Treffen mit Projektleitern teil.	Die Geschäftsleitung (GL) wird regelmässig über den Projektfortschritt und aufgetretende Probleme informiert und in wichtige Projektentscheide einbezogen; dazu trifft sie die Projektleiter oder nimmt aktiv an den Projektfortschrittssitzungen teil.	**3**	**4**	**3**	**3**	**1**	**3**	**1**	**3**	**2**	**3**	**2**	**3**	**3**	**3**	**2.14**	**3.14**

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Bedarfsanalyse / Anwenderbeteiligung	Neue IT-Systeme werden ohne Einbezug aller relevanten Anwendergruppen primär auf Grund von Wünschen und Vorstellungen einzelner Kreise konzipiert.	Neue IT-Systeme werden primär durch die IT-Abteilung auf der Basis von Wünschen und Vorstellungen von Fachbereichen konzipiert. Einzelne Anwendergruppen werden zur Klärung von Detailfragen zugezogen.	Entwicklung/Beschaffung von neuen IT-Systemen ist zum Teil formal geregelt. Neue Systeme werden primär von der IT-Abteilung konzipiert, wobei die verschiedenen Anwendergruppen frühzeitig zur Bedarfsabklärung und -steuerung einbezogen werden.	Es existiert ein umfassender formaler Entwicklungs-/ Beschaffungsprozess für IT-Systeme. Vertreter aller Anwendergruppen sind von Anfang an in den Prozess involviert und verantwortlich für die Vollständigkeit der Spezifikation. Bedarfs-/Spezifikationsänderungen werden durch die Anwendervertreter proaktiv gesteuert.	**4**	**4**	**2**	**3**	**2**	**3**	**2**	**3**	**2**	**3**	**3**	**3**	**3**	**4**	**2.57**	**3.29**
Kosten- / Nutzenanalyse	Projekte werden initiiert, ohne dass Kosten-/Nutzenanalysen durchgeführt werden.	Projekte werden ad-hoc auf Grund von aktuellen Anforderungen von Fachbereichen oder der Geschäftsleitung initiiert, wobei Kosten-/ Nutzenschätzungen auf optimistischen Wunschvorstellungen ohne belegbares Zahlenmaterial basieren. Erforderliche Anpassungen bei anderen Projekten werden kaum erkannt und ausgewiesen.	Projekte werden auf der Basis von nachgewiesenen Bedürfnissen initiiert. Kosten werden quantitativ, der Nutzen eher qualitativ geschätzt. Die Auswirkungen des Projekts auf offensichtlich betroffene andere Anwendungen werden analysiert und Folgekosten werden berücksichtigt.	Projekte entstehen auf der Basis der strategischen ITPlanung des Unternehmens und einer vollständigen Kosten-/Nutzenanalyse (Business Case). Die Zielerreichung wird nach Projektabschluss systematisch gemessen und ausgewertet.	**3**	**4**	**2**	**4**	**2**	**3**	**2**	**2**	**1**	**3**	**2**	**3**	**2**	**4**	**2.00**	**3.29**
Durchschnitt																			**2.07**	**2.98**

Detailed Results – Testing

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	Maturitätsstufe 2	Maturitätsstufe 3	Maturitätsstufe 4	M	I	M	I	M	I	M	I	M	I	M	I	M	I	M	I
Trennung Entwicklung / Produktion	Es existiert keine Testumgebung. Anwendungen werden direkt in die Produktionsumgebung eingespielt und live getestet.	Es existiert keine von der produktiven Umgebung ausreichend getrennte Umgebung für Entwicklung und Test von Anwendungen.	Für einzelne wichtige Anwendungen existieren von der Produktion getrennte Entwicklungs- und Testumgebungen.	Neben der Entwicklungsexistiert eine separate Testumgebung, die von der Produktionsumgebung vollständig getrennt ist. Sämtliche Anwendungen können dort vor ihrer Produktionseinführung gefahrlos getestet werden.	3	4	3	3	3	3	1	2	1	2	1	3	1	3	**1.86**	**2.86**
Kennzeichnung von Systemumgebungen	Die verfügbaren Systemumgebungen sind weder physisch noch logisch getrennt.	Die verfügbaren Systemumgebungen (Entwicklung/ Test/Produktion) sind nicht dokumentiert und weder physisch noch logisch als dedizierte Systemumgebungen erkennbar.	Die verfügbaren Systemumgebungen (Entwicklung/ Test/Produktion) sind zwar dokumentiert, aber weder physisch noch logisch als dedizierte Systemumgebungen erkennbar.	Die verfügbaren Systemumgebungen (Entwicklung/ Test/Produktion) sind dokumentiert. Sie sind sowohl physisch (z.B. mittels Beschriftung) als auch logisch (z.B. Bildschirmhintergrund- oder Textfarbe) klar erkennbar einem bestimmten Typ von Systemumgebung zugeordnet.	3	3	3	3	4	3	1	2	1	2	1	3	2	3	**2.14**	**2.71**
Vollständigkeit von Tests	Testplanung, -durchführung und -dokumentation werden kaum durchgeführt.	Tests sind nicht formalisiert; Testplanung, -durchführung und -dokumentation folgen keinen konkreten Richtlinien.	Tests sind formalisiert; Testplanung, -durchführung und -dokumentation folgen rudimentären Richtlinien. Test werden in der Regel in den meisten (späten) Projektphasen durchgeführt; dies wird jedoch nicht zwingend durchgesetzt und überwacht.	Tests sind formalisiert; Testplanung, -durchführung und -dokumentation folgen in allen Entwicklungsphasen klaren Richtlinien bezüglich Umfang und Vollständigkeit und beziehen sämtliche Fachstellen inkl. Anwenderbereich mit ein. Ausreichend umfangreiche Einzel- und Kettentests werden vollständig und korrekt durchgeführt, was permanent überwacht und regelmässig überprüft wird.	2	3	2	3	3	3	2	3	1	2	2	3	2	3	**2.00**	**2.86**
Verträglichkeitstests	Vor Produktionseinführung von neuen oder geänderten Anwendungen werden keine Tests hinsichtlich der Verträglichkeit für die Umgebung durchgeführt.	Vor Produktionseinführung von neuen und geänderten Anwendungen werden nur rudimentäre Tests hinsichtlich der Verträglichkeit für die bestehende Umgebung durchgeführt.	Die wichtigsten Schnittstellen von neuen und geänderten Anwendungen zu den Umsystemen werden Tests unterzogen. Die Ergebnisse dieser Tests werden jedoch nicht immer systematisch dokumentiert und archiviert.	Es bestehen formalisierte Prozesse für die Durchführung von Verträglichkeitstest neuer oder geänderter Anwendungen für die bestehenden Umgebungen (u.a. Schnittstellen). Die Ergebnisse, die aufgetretenen Fehler und die entsprechenden Lösungen/Korrekturmassnahmen werden systematisch dokumentiert und archiviert, was permanent überwacht und regelmässig überprüft wird.	3	4	3	4	3	3	2	2	1	2	1	3	2	3	**2.14**	**3.00**
Durchschnitt																			**2.04**	**2.86**

Detailed Results – Policies

Kriterium	**Description of Maturity**				**A**		**B**		**C**		**D**		**E**		**F**		**G**		**Durchschnitt**	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Benutzer-Richtlinien Virenschutz	Es gibt keine Anwender-Richtlinien zur Viren-Prävention. Es gibt keine spezifische Ausbildung für Anwender z.B. zum Umgang mit externen Datenträgern, Mail-Anhängen, Internet-Zugriff und unbekannten Downloads.	Es gibt informelle Anwender-Richtlinien zur Viren-Prävention. Die Benutzer sind zwar informiert, dass z.B. externe Datenträger, Mail-Anhänge, Zugriffe auf zweifelhafte Internet-Seiten und unbekannte Downloads eine Gefahr darstellen; es ist aber kein Nachweis möglich, dass die Mitarbeitenden die Richtlinien auch wirklich einhalten.	Es bestehen formelle Anwender-Richtlinien zur Viren-Prävention. Die Benutzer sind informiert, dass z.B. externe Datenträger, Mail-Anhänge, Zugriffe auf zweifelhafte Internet-Seiten und unbekannte Downloads eine Gefahr darstellen; eine eigentliche Ausbildung hat aber in den letzten drei Jahren nicht stattgefunden. Die Einhaltung der Richtlinien wird nur fallweise überwacht.	Es bestehen formelle Anwender-Richtlinien zur Viren-Prävention. Die Benutzer werden im Rahmen von Ausbildungsveranstaltungen instruiert, wie z.B. mit Datenträgern, Mail-Anhängen und unbekannten Downloads umzugehen ist. Die Einhaltung der Richtlinien wird permanent überwacht und periodisch kontrolliert.	**3**	**3**	**3**	**4**	**1**	**3**	**2**	**2**	**1**	**4**	**2**	**4**	**3**	**4**	**2.14**	**3.43**
Verwendung von Internet / E-Mail	Es bestehen keine Anwender-Richtlinien hinsichtlich der Nutzung von Internet und E-Mail. Die Mitarbeitenden werden bezüglich der Risiken bei der Nutzung des Internets und E-Mails nicht sensibilisiert. Internet- und E-Mail-Aktivitäten werden nicht protokolliert und nicht überwacht.	Es bestehen Hinweise hinsichtlich der Nutzung von Internet und E-Mail, und die Mitarbeitenden werden bezüglich der Risiken bei der Nutzung des Internets und E-Mails sensibilisiert. Internet- und E-Mail-Aktivitäten werden weder protokolliert noch anderweitig überwacht und analysiert.	Es bestehen Anwender-Richtlinien hinsichtlich der Nutzung von Internet und E-Mail. Die Mitarbeitenden werden bezüglich der Risiken bei der Nutzung des Internets und E-Mails nachhaltig sensibilisiert. Die Internet- und E-Mail-Aktivitäten werden zwar protokolliert, aber nicht weiter überwacht und analysiert.	Es bestehen formelle Anwender-Richtlinien hinsichtlich der Nutzung von Internet und E-Mail sowie formelle Verfahren für die regelmässige Sensibilisierung sämtlicher Mitarbeitenden mit Zugang zu Computern bezüglich der Risiken bei der Nutzung des Internets und E-Mails. Das E-Mail und Internet-Verhalten wird permanent aufgezeichnet und bezüglich unlauterer oder risikobehafteter Aktivitäten (und Einhaltung des Persönlichkeitsschutzes) analysiert.	**3**	**3**	**3**	**4**	**2**	**3**	**2**	**2**	**1**	**2**	**1**	**3**	**2**	**3**	**2.00**	**2.86**
Archivierung	Es gibt keine Anwender-Richtlinien zur Regelung von Aufbewahrung, Archivierung und Vernichtung von Unterlagen.	Es bestehen informelle Anwender-Richtlinien und Verfahren zur Regelung von Aufbewahrung, Archivierung und Vernichtung von Unterlagen. Es ist aber kein Nachweis möglich, dass die Mitarbeitenden die Richtlinien auch wirklich einhalten.	Es bestehen Anwender-Richtlinien und Verfahren für die Aufbewahrung, Archivierung und Vernichtung von Unterlagen. Die Einhaltung der Richtlinien wird aber nur fallweise überwacht.	Es bestehen formelle Anwender-Richtlinien sowie formelle Verfahren für die Aufbewahrung, Archivierung und Vernichtung von Unterlagen; deren Einhaltung wird überwacht und periodisch kontrolliert.	**3**	**3**	**3**	**3**	**2**	**3**	**1**	**3**	**1**	**2**	**1**	**2**	**2**	**3**	**1.86**	**2.71**
Durchschnitt																			**2.00**	**3.00**

Detailed Results – Training

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Anwender-Handbuch und Dokumentation	Die Benutzer verfügen über keine Benutzer-Handbücher für die verwendeten Anwendungen.	Es stehen nur informelle Benutzer-Handbücher einiger Anwendungen zur Verfügung; in zahlreichen Fällen sind die vorhandenen Dokumentationen aber unvollständig oder nicht aktuell.	Es stehen ausführliche Benutzer-Handbücher von relevanten Anwendungen zur Verfügung; deren Aktualität und Vollständigkeit kann jedoch nicht immer sichergestellt werden.	Es besteht ein umfassendes formelles Verfahren für die Benutzer-Handbücher und Dokumentation von sämtlichen Anwendungen. Die Dokumentationen werden zwingend bereitgehalten und aktuell nachgeführt.	**2**	**3**	**3**	**3**	**3**	**3**	**1**	**3**	**2**	**3**	**2**	**2**	**3**	**3**	**2.29**	**2.86**
Informatikschulungen	Die Anwender erhalten keinerlei Schulung.	Die Anwender werden nach dem Prinzip "learning by doing" geschult; für einzelnen Anwendungen bestehen eigentliche Schulungen.	Es besteht ein Schulungsprogramm, um Mitarbeitende in der korrekten und sicheren Benutzung einer Anwendung zu schulen; diese Ausbildung erfolgt jedoch nicht zwingend vor der erstmaligen Verwendung dieser Anwendung und ist nicht an die spezifischen Bedürfnisse der Anwender und Sicherheitsanforderungen des Unternehmens angepasst.	Ein formelles Schulungsprogramm und entsprechende Verfahren stellen sicher, dass sämtliche Anwender gemäss ihren spezifischen Bedürfnissen, ihrem Kenntnisstand sowie den Sicherheitsanforderungen des Unternehmens systematisch in der korrekten und sicheren Benutzung der Anwendungen geschult werden, bevor sie damit eigenständig arbeiten.	**3**	**4**	**3**	**3**	**2**	**3**	**2**	**3**	**2**	**2**	**2**	**3**	**2**	**3**	**2.29**	**3.00**
Durchschnitt																			**2.29**	**2.93**

Detailed Results – Access Control

Kriterium	**Description of Maturity**				**A**		**B**		**C**		**D**		**E**		**F**		**G**		**Durchschnitt**	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Anwenderprofile	Es bestehen keine auf Rollen basierenden Berechtigungsprofile.	Es bestehen vereinzelte Anwendungen mit auf Rollen basierenden Berechtigungsprofile.	Es besteht ein Berechtigungskonzept mit klaren Rollen und auf Rollen basierende Berechtigungsprofile; umgesetzt ist dieses jedoch nur für bestimmte Anwendungen und Funktionen.	Es besteht ein generelles Berechtigungskonzept mit klaren Rollen und auf den Rollen basierende Berechtigungsprofile. Mitarbeitenden werden entsprechend ihrer Funktion und/oder Stellenbeschreibung 1-n Profile zugeordnet; die Vergabe von Einzelberechtigungen ist nur in Ausnahmefällen notwendig.	**4**	**4**	**3**	**4**	**3**	**3**	**2**	**3**	**1**	**3**	**2**	**3**	**2**	**4**	**2.43**	**3.43**
Verwaltung der Zugangsberechtigungen	Es bestehen keine eigentlichen Verfahren, welche sicherstellen, dass Berechtigungen korrekt erfasst und aktualisiert werden und insbesondere die Berechtigungen von austretenden Mitarbeitern zeitnah gelöscht werden.	Die Verfahren für die Verwaltung von Berechtigungen sind informell; Benutzeridentifikationen und Zugriffsrechte werden ad hoc beim System-Administrator bestellt.	Die Verfahren für die Verwaltung von Berechtigungen sind dokumentiert und mehrheitlich bekannt, so dass die Zugriffsberechtigungen eines Mitarbeiters bei Eintritt gemäss seiner Funktion erstellt und bei dessen Austritt wieder gelöscht werden; der Zugriff auf die Berechtigungsverwaltung ist auf wenige Personen eingeschränkt. Es finden jedoch keine weiteren Überprüfungen statt, um sicherzustellen, dass unbenutzte Konten gelöscht und nicht mehr benötigte Zugriffsrechte entfernt werden.	Es bestehen schriftlich festgehaltene Verfahren für Verwaltung von Berechtigungen, der sicherstellt, dass die Zugriffsberechtigungen eines Mitarbeiters bei Eintritt gemäss seiner Funktion erstellt, periodisch aktualisiert und bei dessen Austritt gelöscht werden. Der Zugriff auf die Berechtigungsverwaltung ist organisatorisch wie technisch strikt auf wenige Personen eingeschränkt. Die Einhaltung der Verfahren wird permanent überwacht und periodisch kontrolliert; Berechtigungen selbst werden regelmässig überprüft, um sicherzustellen, dass unbenutzte Konten nicht mehr aktiv sind und nicht mehr benötigte Zugriffsrechte entfernt wurden.	**3**	**3**	**3**	**4**	**3**	**3**	**1**	**3**	**1**	**3**	**1**	**3**	**2**	**4**	**2.00**	**3.29**

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	Maturitätsstufe 2	Maturitätsstufe 3	Maturitätsstufe 4	M	I	M	I	M	I	M	I	M	I	M	I	M	I	M	I
Unpersönliche Benutzerkonten	Unpersönliche Benutzerkonten werden auch für alltägliche Geschäfts- oder IT-Aktivitäten verwendet, ohne dass dies speziell überwacht wird.	Unpersönliche Benutzerkonten werden fallweise eingesetzt, ohne dass sie systematisch auf ihre Notwendigkeit überprüft werden.	Es ist dokumentiert, in welchen Fällen unpersönliche Benutzerkonten verwendet werden dürfen. Der Zugang dazu ist auf wenige Personen beschränkt; die Rückverfolgung auf die jeweilige Person ist jedoch nicht möglich. Eine periodische Überprüfung auf ihre Notwendigkeit findet nicht statt.	Ein formelles Verfahren stellt sicher, dass unpersönliche Benutzerkonten nur in Ausnahmefällen und mit vorgängigem Einverständnis einer dafür zuständigen Stelle verwendet werden. Unpersönliche Benutzerkonten können von Mitarbeitenden nur über eine vorgängige persönliche Authentifizierung verwendet werden, so dass die Nachvollziehbarkeit sichergestellt ist. Unpersönliche Benutzerkonten werden periodisch auf ihre Notwendigkeit überprüft	**3**	**3**	**3**	**2**	**2**	**2**	**3**	**3**	**1**	**3**	**2**	**3**	**2**	**3**	**2.29**	**2.71**
Authentisierung (mit Passwörtern)	Für die Verwendung von Passwörtern bestehen keinerlei (technische/konzeptionelle) Vorgaben. Wichtige oder besonders exponierte Systeme sind nicht mit Zwei-Faktor-Authentisierungen geschützt.	Der Zugriff auf Systeme und Anwendungen ist grundsätzlich mit Passwörtern geschützt, für einzelne besonders exponierte Systeme gibt es Zwei-Faktor Authentisierungen. Der periodische Passwort-Wechsel wird mindestens 1x pro Jahr erzwungen, jedoch können Benutzer beliebige Passwörter wählen.	Die Verfahren für die Authentisierung von Benutzerkennungen sind dokumentiert sowie grundsätzlich sicher aufgesetzt. Für wichtige oder besonders exponierte Systeme sind Zwei-Faktor-Authentisierungen vorhanden. Der periodische Passwort-Wechsel (mindestens 2x pro Jahr) sowie eine minimale Passwort-Syntax wird erzwungen.	Ein schriftlich festgehaltenes Verfahren stellt sicher, dass für die Authentisierung von Benutzerkennungen ausreichend sichere Verfahren verwendet werden; wichtige oder besonders exponierte Systeme werden mit einer Zwei-Faktor-Authentisierung geschützt. Bei der Verwendung von Passwörtern wird von den Systemen eine starke Passwort-Syntax sowie der periodische Wechsel von Passwörtern erzwungen.	**2**	**3**	**2**	**3**	**3**	**4**	**2**	**2**	**1**	**2**	**1**	**3**	**2**	**3**	**1.86**	**2.86**
Sensibilisierung zum Umgang mit Passwörtern	Es findet keine Sensibilisierung der Mitarbeitenden bezüglich dem sicheren Umgang mit Passwörtern statt. Passwörter werden kaum geändert und häufiger an andere Personen weitergegeben.	Die Mitarbeitenden wurden mindestens einmal (z.B. anlässlich ihrer Einstellung) bezüglich dem sicheren Umgang mit Passwörtern sensibilisiert. Es werden einfach zu erratende Passwörter benutzt, Passwörter werden nicht regelmässig geändert oder werden anderen Benutzern bekannt gegeben.	Die Mitarbeitenden werden ab und zu hinsichtlich der Wahl von starken Passwörtern und dem sicheren Umgang mit ihnen sensibilisiert, jedoch wird ihr Ausbildungsstand nicht in irgendeiner Form ermittelt und festgehalten. Verstösse gegen entsprechende Anweisungen werden nicht zwingend disziplinarisch verfolgt.	Ein schriftlich festgehaltenes Verfahren stellt sicher, dass alle Mitarbeitenden regelmässig hinsichtlich der Wahl von starken Passwörtern und dem sicheren Umgang mit ihnen sensibilisiert werden. Alle Benutzer kennen ihre Verantwortung beim Umgang mit Passwörtern; ihr Ausbildungsstand sowie die Einhaltung wird kontrolliert; Verstösse werden disziplinarisch verfolgt.	**2**	**3**	**2**	**4**	**2**	**3**	**2**	**2**	**1**	**2**	**1**	**3**	**2**	**3**	**1.71**	**2.86**
Durchschnitt																			**2.06**	**3.03**

Detailed Results – Security

Kriterium	**Description of Maturity**				**A**		**B**		**C**		**D**		**E**		**F**		**G**		**Durchschnitt**	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Umgang mit vertraulichen Daten	Es gibt keine Richtlinien für den Umgang mit vertraulichen Daten. Server und Daten sind nicht geschützt. Unerlaubte Zugriffe können nicht erkannt werden.	Es bestehen informelle Benutzer-Richtlinien für den Umgang mit vertraulichen Daten; es ist aber kein Nachweis möglich, dass die Mitarbeitenden diese Richtlinien auch einhalten. Server und Daten sind nicht speziell geschützt. Unerlaubte Zugriffe können nicht erkannt werden.	Es bestehen Benutzer-Richtlinien für den Umgang mit vertraulichen Daten. Die Einhaltung der Richtlinien wird aber nur fallweise überwacht. Verschlüsselungsverfahren für vertrauliche Daten und speziell geschützte Server existieren, werden aber nicht konsequent eingesetzt. Unerlaubte Zugriffe auf vertrauliche Daten können teilweise erkannt und rückverfolgt werden.	Es bestehen formelle Benutzer-Richtlinien für den Umgang mit vertraulichen Daten und die Benutzer sind dementsprechend ausgebildet. Vertrauliche Daten sind verschlüsselt oder befinden sich auf speziell geschützten Servern. Zugriffe auf vertrauliche Daten werden vollständig protokolliert und periodisch kontrolliert.	**3**	**4**	**2**	**3**	**2**	**4**	**2**	**1**	**2**	**3**	**2**	**3**	**3**	**4**	**2.29**	**3.14**
Anwendersensibilisierung	Es findet keinerlei Sensibilisierung bzw. Schulung der Anwender hinsichtlich der Informations- und ITSicherheit statt.	Eine informelle Anleitung zur korrekten Nutzung der Informationssysteme und zur Informations- und IT-Sicherheit ist vorhanden; sie wird allerdings nicht konsequent kommuniziert. Eine Schulung der Anwender findet nicht statt.	Es bestehen klare und verbindliche Anleitungen zur korrekten Nutzung der Informationssysteme und zur Informations- und IT-Sicherheit, welche den Mitarbeitenden bei Eintritt in das Unternehmen ausgehändigt werden. Eine Schulung gibt es zum grössten Teil für Neu-Eintretende; andere Mitarbeiter werden nicht systematisch geschult.	Eine formelle Anleitung zur korrekten Nutzung der Informationssysteme und zur Informations- und ITSicherheit besteht und wird aktiv an sämtliche Benutzer verteilt. Systematische Schulungen finden zielgruppen- und funktionsgerecht in regelmässigen Abständen statt und werden nachweislich vom grössten Teil der Mitarbeitenden besucht. Ergänzende Sensibilisierungs-Massnahmen werden geplant umgesetzt.	**2**	**3**	**3**	**3**	**2**	**4**	**1**	**2**	**1**	**3**	**2**	**3**	**2**	**3**	**1.86**	**3.00**
Virenschutzprogramme	Server und Arbeitsplätze (Clients) verfügen über keinerlei Virenschutzprogramme.	Server und Arbeitsplätze (Clients) verfügen teilweise über ein Virenschutzprogramm; dieses wird aber nicht regelmässig aktualisiert.	Server und Arbeitsplätze (Clients) verfügen über ein Virenschutzprogramm; dieses wird aber nicht täglich aktualisiert.	Das Unternehmen verfügt über ein täglich online aktualisiertes Virenschutzprogramm, das auf allen Servern und Arbeitsplätzen installiert ist und von den Benutzern nicht deaktiviert werden kann.	**3**	**3**	**4**	**3**	**4**	**4**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**3.71**	**3.71**

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Administrationsrechte am Arbeitsplatzrechner	Es besteht kein Konzept für die Vergabe von Administratorberechtigungen; einzelne Benutzer in Fachbereichen verfügen an ihren Arbeitsplätzen über Administratorberechtigungen, wodurch Software ohne Genehmigung eines Verantwortlichen installiert werden kann.	Es besteht ein informelles Konzept für die Vergabe von Administrator-Berechtigungen. Einzelne registrierte Benutzer verfügen an ihren Arbeitsplätzen über Administratorberechtigungen, wodurch Software ohne Genehmigung eines Verantwortlichen installiert werden kann.	Es besteht ein formelles Konzept für die Vergabe von Administrator-Berechtigungen. Einzelne registrierte Benutzer verfügen an ihren Arbeitsplätzen über Administratorberechtigungen, wodurch Softwareinstallationen ohne Genehmigung eines Verantwortlichen möglich sind. Die Benutzer sind jedoch verpflichtet, die Software vor der Installation genehmigen und prüfen zu lassen.	Es besteht ein formelles Konzept für die Vergabe von Administrator-Berechtigungen. Kein Benutzer verfügt über Administrationsberechtigungen am Arbeitsplatz. Eine Softwareinstallation muss durch ein formelles Antragswesen von verantwortlicher Stelle bewilligt werden. Die Software wird nach vorgängiger Prüfung von den zuständigen und berechtigten Fachspezialisten auf den entsprechenden Arbeitsplätzen installiert.	**4**	**4**	**2**	**4**	**2**	**4**	**2**	**2**	**1**	**3**	**1**	**3**	**2**	**4**	**2.00**	**3.43**
Netzwerkschutz	Es besteht kein Konzept, das den Netzwerk-Perimeterschutz regelt; das Netzwerk verfügt über keine erkennbaren Schutzmassnahmen; ein- und ausgehende Datenströme werden weder registiert noch weiter überwacht.	Es bestehen grundlegende Sicherheitsmassnahmen zum Schutz der Verbindungen zwischen dem internen Netzwerk und der Aussenwelt. Ein- und ausgehende Datenströme werden weder registriert noch weiter überwacht.	Alle Netzwerkverbindungen zwischen dem internen Netzwerk und der Aussenwelt werden basierend auf einem klaren Konzept geschützt; ein- und ausgehende Datenströme werden registriert und permanent überwacht.	Alle Netzwerkverbindungen zwischen dem internen Netzwerk und der Aussenwelt werden basierend auf einem klaren Konzept geschützt; die Anwenderverbindungen werden überwacht. Die Netzwerkverbindungen werden periodisch durch unabhängige Experten auf Schwachstellen und Verwundbarkeiten untersucht.	**2**	**3**	**2**	**4**	**2**	**4**	**1**	**2**	**1**	**3**	**1**	**3**	**4**	**4**	**1.86**	**3.29**
Remote Access	Es besteht kein Konzept für die Vergabe von Fernzugriff; es bestehen Fernzugriffskonten, von denen bisher niemand etwas wusste.	Es besteht ein informelles Konzept für die Vergabe von Fernzugriff; jedoch wird es nicht systematisch umgesetzt. Fernzugriffe aus externen Netzen auf die ITInfrastruktur (z.B. Fernwartung, Bereitschaftsdienst) werden nicht auf Auftretenshäufigkeit, Herkunft und Notwendigkeit geprüft.	Es besteht ein formelles Konzept für die Vergabe von Fernzugriff. Fernzugriffe aus externen Netzen auf die IT-Infrastruktur (z.B. Fernwartung, Bereitschaftdienst) werden teilweise protokolliert, jedoch nicht systematisch auf Auftretenshäufigkeit, Herkunft und Notwendigkeit geprüft.	Es besteht ein formelles Konzept für die Vergabe von Fernzugriff. Die Zugriffe werden systematisch protokolliert und periodisch ausgewertet. Fernzugriffe werden regelmässig, mindestens einmal jährlich, von unabhängiger Stelle auf Auftretenshäufigkeit, Herkunft und Notwendigkeit geprüft.	**3**	**4**	**3**	**4**	**2**	**4**	**1**	**1**	**1**	**3**	**2**	**3**	**4**	**4**	**2.29**	**3.29**
Durchschnitt																			**2.33**	**3.31**

Detailed Results – Physical Security

Kriterium	**Description of Maturity**				**A**		**B**		**C**		**D**		**E**		**F**		**G**		**Durchschnitt**	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Brandschutz	Die IT-Infrastruktur ist nicht vor Bränden geschützt und es existieren keine Mittel zur Brandlöschung. In Räumen der IT-Infrastruktur oder in deren unmittelbaren Umgebung befinden sich grosse Brandlasten.	Die IT-Infrastruktur ist nicht speziell vor Bränden geschützt und es existieren nur rudimentäre Mittel zur Brandlöschung. In den Räumen der IT-Infrastruktur oder in deren unmittelbaren Umgebung befinden sich teilweise grosse Brandlasten.	Die IT-Infrastruktur wird trotz der Einhaltung der geltenden Brandschutzbestimmungen nur unzureichend geschützt; IT-spezifische Anforderungen wie spezielle Löschmittel oder die Vermeidung von Brandlasten in der unmittelbaren Umgebung werden nur teilweise erfüllt.	Die IT-Infrastruktur ist durch die Einrichtung von Brandschutzzonen, Brandmeldesystemen und angemessenen Löscheinrichtungen vor den Auswirkungen eines Brandes geschützt. Brennbare Materialien werden weder in den Informatikräumen noch in deren unmittelbaren Umgebung aufbewahrt.	**4**	**4**	**3**	**3**	**1**	**4**	**2**	**2**	**1**	**4**	**3**	**4**	**3**	**4**	**2.43**	**3.57**
Absicherung der Stromversorgung	Das Unternehmen verfügt über keinerlei Schutzmassnahmen vor Stromausfällen und Spannungsschwankungen.	Das Unternehmen verfügt über einen Schutz vor Spannungsschwankungen für die wichtigsten ITEinrichtungen (z.B. Server, Rechenzentrum), aber nur ausnahmsweise über eine unterbrechungsfreie Stromversorgung.	Das Unternehmen verfügt über eine unterbrechungsfreie Stromversorgung und Schutz vor Spannungsschwankungen für die wichtigsten Server und Einrichtungen. Für die Arbeitsplätze selbst gibt es allerdings keine unterbrechungsfreie Stromversorgung.	Das Unternehmen verfügt für die gesamte IT-Infrastruktur (inkl. der wichtigsten Arbeitsplätze) über eine unterbruchsfreie Stromversorgung zur Vermeidung von Schäden infolge von Stromausfällen oder Spannungsschwankungen.	**3**	**3**	**3**	**3**	**3**	**4**	**3**	**3**	**2**	**3**	**2**	**3**	**2**	**3**	**2.57**	**3.14**
Zugang zu den Räumlichkeiten	Personen können die Firmenräumlichkeiten ungehindert betreten und sich frei bewegen, ohne sich am Empfang anzumelden. Die Informatikräume sind unverschlossen und werden nicht überwacht. Ausserhalb der Arbeitszeit sind die Räumlichkeiten nicht durch ein Einbruchmeldesystem abgesichert.	Personen können die Firmenräumlichkeiten ungehindert betreten und sich frei bewegen, ohne sich am Empfang anzumelden. Die Informatikräume sind verschlossen, werden aber nicht überwacht. Ausserhalb der Arbeitszeit sind die Räumlichkeiten nicht durch ein Einbruchmeldesystem abgesichert.	Das Unternehmen verfügt über einen Empfang, jedoch nicht über Schleusen oder Durchgangssperren für die Zugangskontrolle zu den Innenräumen. Besucher werden nicht systematisch in internen Zonen begleitet, aber die Informatikräume sind über eine Zugangskontrollsystem abgesichert. Versuchte oder erfolgte Zutritte sind nachvollziehbar.	Alle Räumlichkeiten werden überwacht, Zutritte werden protokolliert. Besucher müssen sich am Empfang anmelden und werden während ihres gesamten Aufenthalts in den Unternehmensräumlichkeiten begleitet. Die Informatikräume sind gesichert; der Zutritt für firmenfremde Personen (Besucher, Wartungstechniker etc.) muss explizit beantragt werden. Fremde Personen werden in Sicherheitszonen permanent überwacht.	**3**	**3**	**2**	**3**	**3**	**4**	**2**	**3**	**1**	**3**	**1**	**3**	**3**	**4**	**2.14**	**3.29**
Durchschnitt																			**2.38**	**3.33**

Detailed Results – Operations

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	Maturitätsstufe 2	Maturitätsstufe 3	Maturitätsstufe 4	M	I	M	I	M	I	M	I	M	I	M	I	M	I	M	I
Aufgaben in Anwendungen	Die Zuständigkeiten und Verantwortlichkeiten im Zusammenhang mit der Nutzung, der Pflege und dem Betrieb der Anwendungen sind nicht festgelegt. Es wird keine Gewaltentrennung auf technischer und organisatorischer Ebene durchgesetzt.	Die Zuständigkeiten und Verantwortlichkeiten im Zusammenhang mit der Nutzung, der Pflege und dem Betrieb der Anwendungen sind den Mitarbeitern grundsätzlich bekannt, aber nicht dokumentiert. Die technische oder organisatorische Gewaltentrennung kann von den Mitarbeitern umgangen werden.	Die Zuständigkeiten und Verantwortlichkeiten im Zusammenhang mit der Nutzung, der Pflege und dem Betrieb der Anwendungen sind festgelegt und dokumentiert; die technische Gewaltentrennung kann jedoch von den Mitarbeitern umgangen werden.	Die Zuständigkeiten und Verantwortlichkeiten im Zusammenhang mit der Nutzung, der Pflege und dem Betrieb der Anwendungen sind formal festgelegt und dokumentiert. Die technische Gewaltentrennung wird regelmässig auf Erfüllung der Anforderungen geprüft.	3	2	2	3	2	3	1	4	1	3	1	3	3	3	1.86	3.00
Betrieb	Für die Funktion des Administrators wurde keine Person abgestellt; Netzwerk und Systeme werden nicht überwacht und gepflegt.	Es wurde ein Administrator bestimmt; dieser hat jedoch noch weitere Funktionen im Betrieb inne und kann sich somit nicht immer um die Systempflege- und Überwachungsaufgaben kümmern.	Es wurde ein Administrator und/oder ein Betriebsteam* bestimmt, welche für Netzund Systempflege zuständig ist/sind. Eine Überwachung findet sporadisch aber nicht täglich statt.	Es wurde ein Administrator und/oder ein Betriebsteam* bestimmt. Netz- und Systempflege- und -überwachungsaufgaben werden täglich und systematisch durchgeführt.	3	4	3	3	3	3	2	3	1	3	2	4	3	4	2.43	3.43
Konfigurationsmanagement	Der Zugriff auf die Konfigurationsdaten von Systemen ist de facto weder durch Verfahren geregelt noch auf berechtigte Personen eingeschränkt.	Die Verfahren für die Änderung der Konfiguration von Systemen sind informell; Änderungen an der Konfiguration von Systemen werden nicht aufgezeichnet.	Die Verfahren für Änderungen an der Konfiguration von Systemen sind dokumentiert und mehrheitlich bekannt und der Zugriff auf berechtigte Personen eingeschränkt. Konfigurationsänderungen werden protokolliert; diese werden aber nur fallweise überprüft.	Es besteht ein formelles Verfahren für Änderungen an der Konfiguration von Systemen; alle Änderungen werden vor ihrer Durchführung verifiziert und dauerhaft dokumentiert. Erfolgte Konfigurationsänderungen werden automatisch erkannt, rapportiert und auf Übereinstimmung mit einem entsprechenden Änderungsauftrag überprüft.	3	4	3	3	2	3	1	4	1	3	2	3	3	4	2.14	3.43
Systemüberwachung & Wartung	System-Komponenten werden kaum überwacht und nur bei grösseren Störungen ausgewechselt.	Es bestehen informelle Verfahren für die Systemüberwachung; eine technische Überwachung wird teilweise durchgeführt und System-Komponenten werden bei Bedarf (reaktiv) ausgewechselt.	Es bestehen formelle Verfahren für die Systemüberwachung; eine technische Überwachung wird durchgeführt und System-Komponenten werden nach einem vordefinierten Plan ausgewechselt. Die relevanten Daten werden teilweise protokolliert und ausgewertet; teilweise werden Benutzerbefragungen durchgeführt.	Es bestehen formelle Verfahren für die Systemüberwachung, die konsequent umgesetzt werden. Die Leistung der wichtigen System-Komponenten wird permanent aufgezeichnet und regelmässig vom für Systemüberwachung zuständigen IT-Verantwortlichen kontrolliert (Ausfälle, Störungen, Reaktionszeit usw.). Befragungen der Benutzer dienen zur Bedarfsermittlung.	2	2	2	3	2	3	2	3	1	3	2	3	3	4	2.00	3.00

Kriterium	**Description of Maturity**				**A**		**B**		**C**		**D**		**E**		**F**		**G**		**Durchschnitt**	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Einsatz von Tools	Für den Betrieb der IT werden kaum Tools eingesetzt.	Für den Betrieb der Informatik werden vereinzelte Tools eingesetzt; deren Einsatz erfolgt aber primär reaktiv und isoliert.	Für den Betrieb der Informatik werden Tools eingesetzt; deren Einsatz ist aber wenig aufeinander abgestimmt und erfolgt häufig reaktiv.	Für den Betrieb der Informatik werden basierend auf einem klaren Konzept Tools eingesetzt. Die verschiedenen Werkzeuge sind klar aufeinander abgestimmt; ihr Einsatz erfolgt geplant und nach klaren Vorgaben.	**3**	**3**	**3**	**4**	**2**	**2**	**2**	**3**	**1**	**2**	**2**	**2**	**3**	**3**	**2.29**	**2.71**
Netzwerküberwachung	Das Netzwerk wird kaum überwacht und es besteht keine klare Verantwortlichkeit für die Netzwerküberwachung.	Einzelne Verbindungs- und Fehlerstatistiken über das Netzwerk und die Netzwerkkompenenten sind verfügbar, werden aber nicht systematisch analysiert.	Verbindungs- und Fehlerstatistiken des Netzwerks und der Netzwerk-Komponenten werden systematisch protokolliert; diese werden jedoch eher situativ (z.B. nach Vorkommnissen) analysiert.	Verbindungs- und Fehlerstatistiken des Netzwerks und von Netzwerk-Komponenten werden basierend auf einem klaren Konzept systematisch und vollständig protokolliert; diese werden regelmässig überprüft und aufgetretene Zwischenfälle systematisch untersucht.	**2**	**4**	**3**	**4**	**2**	**3**	**1**	**3**	**1**	**2**	**1**	**3**	**4**	**3**	**2.00**	**3.14**
Kontrolle der Systemleistung	Es erfolgt keinerlei Kontrolle der Systemleistungen innerhalb des Betriebs.	Es bestehen informelle Verfahren für die Kontrolle der effektiven Systemleistung. Die Beobachtungen werden nicht festgehalten.	Es bestehen formelle Verfahren für die Kontrolle der effektiven Systemleistung; die Aufzeichnung erfolgt automatisch. Eine Auswertung wird nur fallweise erstellt.	Es bestehen formelle Verfahren für die Kontrolle der effektiven Systemleistung; Störungen, Ausfälle und Reaktionszeiten der Anwendungen und Systeme werden automatisch erkannt und konsequent abgeklärt. Eine Zusammenfassung der Fehler und der eingeleiteten Störungsbehebungsmassnahmen ist verfügbar.	**2**	**3**	**2**	**4**	**3**	**3**	**2**	**2**	**1**	**3**	**2**	**3**	**3**	**3**	**2.14**	**3.00**
Durchschnitt																			**2.12**	**3.10**

Detailed Results – Problem Management

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Umgang mit Fehlern	Es gibt keine Verfahren zum Umgang mit Störungen oder Fehlern.	Es bestehen wenig formelle Verfahren zum Umgang mit Störungen und Fehlern. Fehler werden nicht systematisch aufgezeichnet und sind kaum rekonstruierbar. Problem-Berichte werden erstellt.	Verfahren für den Umgang mit Störungen und Fehlern sind für die meisten Systeme weitgehend geregelt; die Einhaltung der Verfahren wird aber nur fallweise überprüft. Störungen werden aufgezeichnet, aber nur fallweise ausgewertet.	Es gibt formelle Verfahren für den Umgang mit Störungen und Fehlern. Ereignisse sind lückenlos nachvollziehbar und werden systematisch abgeklärt. Die Fehlerberichte werden systematisch archiviert.	**2**	**3**	**2**	**3**	**2**	**2**	**2**	**3**	**1**	**3**	**2**	**4**	**3**	**4**	**2.00**	**3.14**
Help-Desk	Es besteht kein Helpdesk. Benutzer gehen direkt auf Mitarbeiter der IT zu und melden ihre Probleme informell.	Es besteht ein Helpdesk; dieser ist aber aus unterschiedlichen Gründen (Ressourcen, Knowhow, etc.) nicht in der Lage, alle Mitarbeiteranfragen zu bewältigen. Informelle Kontakte zwischen Benutzern und IT werden als Alternative zum Help Desk genutzt.	Ein spezieller Benutzer-Helpdesk steht während der gesamten Arbeitszeit zur Verfügung und ist in der Lage, die Mitarbeiteranfragen zu bewältigen. Informelle Kontakte zwischen Benutzern und IT werden auf den Help Desk weiter vermittelt.	Ein spezieller Benutzer-Helpdesk ist während der gesamten Arbeitszeit verfügbar und ist quantitativ wie qualitativ in der Lage, die Mitarbeiteranfragen zu bewältigen. Anfragen, die erkannten Probleme wie die gemachten Lösungen werden in einem System systematisch erfasst und zur proaktiven Verbesserung eingesetzt.	**4**	**4**	**3**	**2**	**3**	**4**	**1**	**3**	**1**	**2**	**1**	**2**	**3**	**3**	**2.29**	**2.86**
Durchschnitt																			**2.14**	**3.00**

Detailed Results – Backup

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
Sicherungskonzept	Es existiert kein Datensicherun	Es besteht ein informelles Datensicherungskonzept; es ist jedoch nicht schriftlich festgehalten.	Es besteht ein schriftlich festgehaltenes Datensicherungskonzept, das klar regelt, welche Daten zu welchem Zeitpunkt, in welchem Umfang und in welcher Zahl Generationen gespeichert werden; Aufbewahrungsort und -dauer sind teilweise spezifiziert. Die Einhaltung des Konzepts wird nur fallweise geprüft.	Es besteht ein schriftlich festgehaltenes Datensicherungskonzept, das klar regelt, welche Daten zu welchem Zeitpunkt, in welchem Umfang und in welcher Zahl Generationen gespeichert werden. Die Einhaltung des Konzepts wird regelmässig geprüft.	**4**	**4**	**3**	**4**	**2**	**4**	**2**	**4**	**2**	**4**	**2**	**4**	**4**	**4**	**2.71**	**4.00**
Sicherungsprozess	Es werden keine Datensicherungen durchgeführt.	Es werden keine regelmässigen Datensicherungen durchgeführt und die erstellten Sicherungen werden nicht kontrolliert.	Es werden täglich (oder häufiger) Sicherungen gemäss dem Datensicherungskonzept durchgeführt. Die Durchführung wird protokolliert, aber die Protokolle werden nur fallweise überprüft.	Es werden täglich (oder häufiger) Sicherungen gemäss dem Datensicherungskonzept durchgeführt. Die Durchführung wird protokolliert, und die Protokolle werden nach jeder Sicherung überprüft.	**4**	**4**	**3**	**3**	**3**	**4**	**3**	**4**	**3**	**4**	**3**	**4**	**4**	**4**	**3.29**	**3.86**
Wiederherstellungstest	Es werden keine Tests zum Zurückladen der Sicherungen durchgeführt.	Es werden informelle aber keine systematischen Tests zum Zurückladen der Sicherungen durchgeführt (z.B. auf Initiative der Fachabteilungen).	Tests zum Zurückladen der Daten werden periodisch durchgeführt; ihre Resultate werden protokolliert, aber nur fallweise kontrolliert.	Systematische Tests zum Zurückladen der Sicherungen aller Kernanwendungen werden regelmässig (nicht seltener als 1x pro Monat) durchgeführt; die Resultate werden protokolliert und systematisch kontrolliert.	**2**	**3**	**3**	**4**	**3**	**4**	**1**	**4**	**1**	**4**	**2**	**4**	**4**	**4**	**2.29**	**3.86**

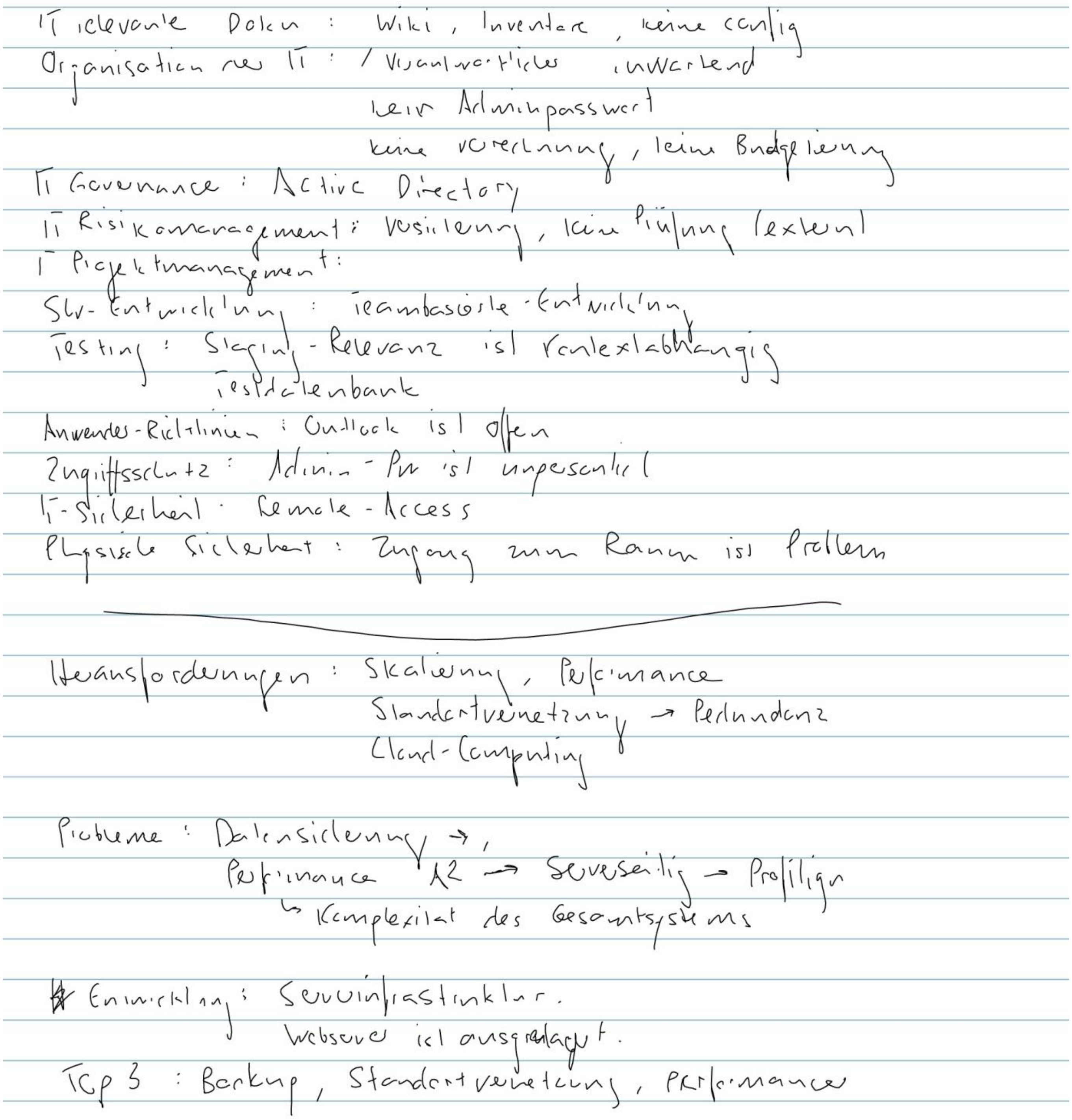
Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	**Maturitätsstufe 2**	**Maturitätsstufe 3**	**Maturitätsstufe 4**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**	**M**	**I**
IT-Notfallplan	Es wurden keine Überlegungen zu einem IT-Notfallplan angestellt.	Überlegungen zur Bestimmung der wichtigsten Daten und der Elemente des Informationssystems, ohne die das Unternehmen seine Geschäftstätigkeit nicht fortführen kann, wurden angestellt. Ein IT-Plan zur Unterstützung der Wiederaufnahme der Geschäftstätigkeit im Schadensfall wurde nicht erstellt.	Überlegungen zur Bestimmung der wichtigsten Daten und der Elemente des Informationssystems, ohne die das Unternehmen seine Geschäftstätigkeit nicht fortführen kann, wurden angestellt. Ein ITPlan zur Wiederaufnahme der Geschäftstätigkeit im Schadensfall wurde erstellt, aber es wurden noch keine konkreten technischen und personellen Vorkehrungen getroffen.	Es wurden Vorkehrungen für die Umsetzung des IT-Notfallplans (z.B. Bereitstellung eines Ausweichstandorts für Notfälle bzw. die Aufbewahrung von Ersatz-Hardware für Störungsfälle) getroffen. Ein IT-Plan zur Wiederaufnahme der Geschäftstätigkeit wurde formalisiert und enthält die Rollen der Beteiligten und die prioritär wiederherzustellenden Systeme. Der Plan wird regelmässig getestet und ist einsatzbereit.	**2**	**3**	**2**	**3**	**3**	**3**	**1**	**4**	**1**	**3**	**1**	**4**	**3**	**4**	**1.86**	**3.43**
Datenauslagerung	Datensicherungen werden nicht ausserhalb des Unternehmens aufbewahrt.	Datensicherungen werden ausgelagert, der Prozess ist aber nicht geregelt und nicht dokumentiert. Der Zugriff auf die Speichermedien ist für das Unternehmen nicht jederzeit gewährleistet (z.B. bei Auslagerung in den privaten Räumlichkeiten eines Mitarbeiters).	Es besteht ein schriftlich festgehaltenes Konzept für die Auslagerung von Datensicherungen, das vollständig umgesetzt ist. Die Auslagerung wird protokolliert, das Protokoll aber nur fallweise überprüft. Der Zugriff auf die Speichermedien innerhalb der definierten Zeitspanne ist für das Unternehmen aber nicht immer gewährleistet (z.B. bei Auslagerung in privaten Räumlichkeiten eines Mitarbeiters).	Es besteht ein schriftlich festgehaltenes Konzept für die Auslagerung von Datensicherungen, das vollständig umgesetzt ist. Die Auslagerung wird protokolliert, und das Protokoll wird systematisch überprüft. Der Zugriff auf die Speichermedien innerhalb der definierten Zeitspanne ist für das Unternehmen jederzeit gewährleistet, durch einen Prozess sichergestellt und dokumentiert.	**3**	**4**	**4**	**2**	**3**	**3**	**2**	**4**	**2**	**4**	**3**	**3**	**4**	**4**	**3.00**	**3.43**
Durchschnitt																			**2.63**	**3.71**

Detailed Results – Outsourcing

Kriterium	Description of Maturity				A		B		C		D		E		F		G		Durchschnitt	
	Maturitätsstufe 1	Maturitätsstufe 2	Maturitätsstufe 3	Maturitätsstufe 4	M	I	M	I	M	I	M	I	M	I	M	I	M	I	M	I
Outsourcing-Vereinbarungen	Es bestehen keine Outsourcing-Vereinbarungen mit den externen Dienstleistern.	Es bestehen keine Outsourcing-Vereinbarungen mit den externen Dienstleistern.	Leistungen von externen Dienstleistern basieren auf schriftlichen Vereinbarungen, welche die vereinbarten Leistungen beschreiben. Qualität, Sicherheit und Verfügbarkeit sind jedoch nicht umfassend geregelt. Es gibt informelle Verfahren zur Überwachung der Leistung und zu deren Verbesserung bei Nichteinhaltung der Vereinbarungen; Modalitäten zur Vertragsauflösung sind teilweise festgelegt.	Leistungen von externen Dienstleistern basieren auf Service Level Agreements und klaren Verträgen, die die Qualität der Leistungen, die Verfügbarkeit sowie Sicherheit und Verfügbarkeit sicherstellen. Die Einhaltung der Vereinbarung wird laufend überwacht. Bei A bweichungen werden gezielt Massnahmen getroffen; Modalitäten zur Vertragsauflösung sind klar festgelegt.	**3**	**3**	**2**	**2**	**4**	**4**	**1**	**3**	**2**	**3**	**2**	**3**	**3**	**3**	**2.43**	**3.00**
Kontrollmöglichkeit beim Outsourcing-Partner	Die Wartungs- und Supporteinsätze der externen Dienstleister werden sporadisch protokolliert; das Ergebnis ihrer Leistungen wird jedoch nicht mit dem erwarteten Ergebnis verglichen.	Die Leistungen sowie die Sicherheitsmassnahmen sind nur in der Dokumentation des externen Dienstleisters beschrieben. Massnahmen zur Kontrolle der Leistungen und Einhaltung von Sicherheitsanforderungen sind in den Verträgen nicht formal definiert.	Die Leistungen sowie die vom Provider zu erfüllenden Sicherheitsanforderungen sind schriftlich festgelegt. Massnahmen zur Kontrolle der Leistungen und Einhaltung von Sicherheitsanforderungen sind in den Verträgen formal definiert; deren Einhaltung wird aber nicht konkret überprüft. Der externe Dienstleister wird durch eine unabhängige Stelle regelmässig überprüft; der Prüfbericht wird dem Kunden ausgehändigt.	Die Leistungen sowie die vom Provider zu erfüllenden Sicherheitsanforderungen sind detailliert schriftlich festgelegt; Massnahmen zur Kontrolle der Leistungen und Einhaltung von Sicherheitsanforderungen sind in den Verträgen formal definiert und werden umgesetzt. Der externe Dienstleister wird durch eine unabhängige Stelle regelmässig hinsichtlich der in den Verträgen festgehaltenen Zielen überprüft; der Prüfbericht wird dem Kunden ausgehändigt. Er hat das Recht, zusätzliche Prüfungen beim Dienstleister durchzuführen (Right to Audit).	**2**	**3**	**2**	**3**	**2**	**2**	**1**	**3**	**1**	**3**					**1.60**	**2.80**
Überwachung der Support-Tätigkeiten	Die Wartungs- und Supporteinsätze der externen Dienstleister werden nicht überwacht, das Ergebnis ihrer Leistungen wird nicht mit dem erwarteten Ergebnis verglichen.	Die Wartungs- und Supporteinsätze der externen Dienstleister werden sporadisch protokolliert; das Ergebnis ihrer Leistungen wird jedoch nicht mit dem erwarteten Ergebnis verglichen.	Die Wartungs- und Supporteinsätze der externen Dienstleister werden sporadisch protokolliert; das Ergebnis ihrer Leistungen wird jedoch nicht mit dem erwarteten Ergebnis verglichen.	Die Wartungs- und Supporteinsätze der externen Dienstleister werden sporadisch protokolliert; das Ergebnis ihrer Leistungen wird jedoch nicht mit dem erwarteten Ergebnis verglichen.	**2**	**2**	**3**	**2**	**3**	**3**	**1**	**4**	**2**	**3**	**2**	**3**	**2**	**3**	**2.14**	**2.86**
Durchschnitt																			**2.06**	**2.89**

Appendix C – Interviews

Interview with Martin Zurbrüg (Informaticon AG, Thun)



IT relevante Doku : Wiki, Inventare, keine config
Organisation der IT : / Verantwortlicher inwartend
kein Adminpasswort
keine Verrechnung, keine Budgetierung
IT Governance : Active Directory
IT Risikomanagement : Versicherung, keine Prüfung (extern)
IT Projektmanagement :
SW-Entwicklung : teambasierte Entwicklung
Testing : Staging - Relevanz ist kontextabhängig
Testdatenbank
Anwender-Richtlinien : Outlook ist offen
Zugriffsschutz : Admin-PW ist unpersönlich
IT-Sicherheit : Remote-Access
Physische Sicherheit : Zugang zum Raum ist Problem

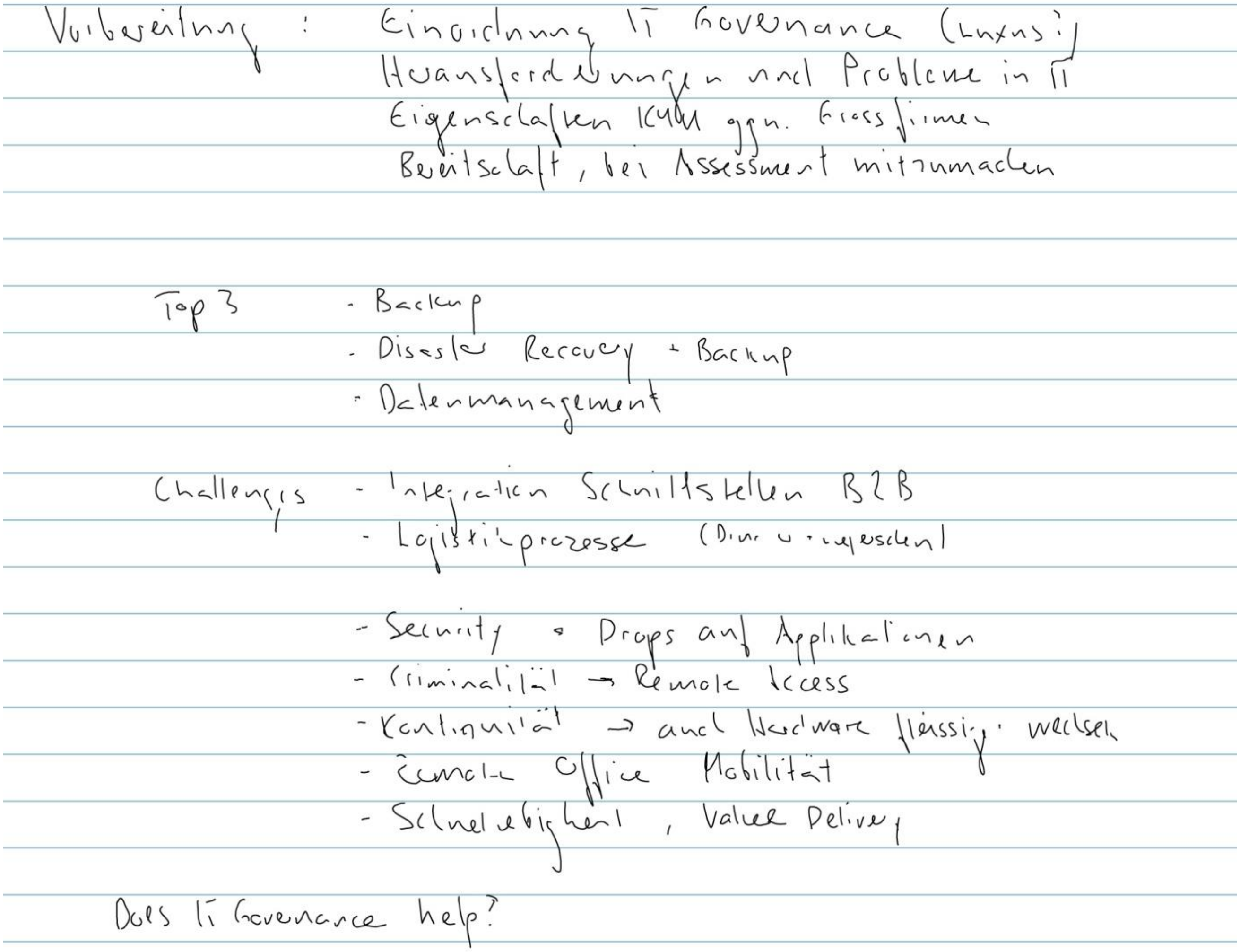
Herausforderungen : Skalierung, Performance
Standortvernetzung → Redundanz
Cloud-Computing

Probleme : Datensicherung →,
Performance A2 → Serverseitig → Profiling
↳ Komplexität des Gesamtsystems

☆ Entwicklung : Serverinfrastruktur.
Webserver ist ausgelagert.
Top 3 : Backup, Standortvernetzung, Performance

Figure 38: Interview notes - Martin Zurbrügg.

Interview with Hugo Bosshard (Studerus AG, Schwerzenbach)



Vorbereitung : Einordnung IT Governance (Luxus?)
Herausforderungen und Probleme in IT
Eigenschaften KMU ggn. Grossfirmen
Bereitschaft, bei Assessment mitzumachen

Top 3
- Backup
- Disaster Recovery + Backup
- Datenmanagement

Challenges
- Integration Schnittstellen B2B
- Logistikprozesse (Dim. u. Lagerscheine)

- Security + Drops auf Applikationen
- Criminalität → Remote Access
- Kontinuität → auch Hardware flüssig. wechseln
- Remote Office Mobilität
- Schnelligkeit, Value Delivery

Does IT Governance help?

Figure 39: Interview notes - Hugo Bosshard.