DEGREE PROJECT

Towards an Integrated Framework for Quality and Information Security Management in Small Companies

Christine Große

Information Security, masters level
2016

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

LULEÅ TEKNISKA UNIVERSITET

List of Contents

List of Contents i
List of Figures iv
List of Tables v
List of Abbreviations vi
Abstract ... .
1 Introduction ..... - 1 -
1. 1 Motivation ..... - 1 -
1. 2 Problem Description ..... - 2 -
1. 3 Research Question and Contribution ..... - 5 -
1. 4 Related Work ..... - 7 -
1. 5 Structure of the Thesis ..... - 8 -
2 Foundation ..... - 9 -
2. 1 Management of Information Systems ..... - 9 -
2. 1. 1 Corporate & IT Governance ..... - 9 -
2. 1. 2 Quality Management ..... - 10 -
2. 1. 3 Information Security Management ..... - 11 -
2. 2 Information Security in MSE ..... - 13 -
2. 2. 1 Threats to Information Security ..... - 13 -
2. 2. 2 Impact of the Violation of Secrecy ..... - 15 -
2. 2. 3 Barriers to Enhanced Information Security ..... - 16 -
2. 3 Modelling ..... - 17 -
2. 3. 1 Model Features ..... - 17 -
2. 3. 2 Model Building ..... - 19 -
2. 3. 3 Reference Model ..... - 20 -
3 Research Process ..... - 23 -
3. 1 Information Systems Research ..... - 23 -
3. 2 Applied Research Method Spectrum ..... - 24 -
3. 2. 1 Analysis – Standards and Good Practices ..... - 24 -
3. 2. 2 Design – Framework and Modelling ..... - 24 -
3. 2. 3 Evaluation and Contribution ..... - 25 -

3. 3 Reference and Process Modelling - 26 -
3. 3. 1 Modelling Approach - 26 -
3. 3. 2 Model Annotation and Tool Support - 27 -
3. 3. 3 Evaluation Criteria for Conceptual Models - 29 -
4 Standards and Good Practices - 31 -
4. 1 COBIT 5 - 31 -
4. 1. 1 Characteristics of COBIT 5 - 31 -
4. 1. 2 Analysis of COBIT 5 - 32 -
4. 1. 3 Interim Summary of COBIT 5 Features - 34 -
4. 2 IT Infrastructure Library (ITIL®) - 35 -
4. 2. 1 Characteristics of ITIL® - 35 -
4. 2. 2 Analysis of ITIL® - 36 -
4. 2. 3 Interim Summary of ITIL® v.3 2011 Features - 38 -
4. 3 ISO 9001 and ISO 27001 - 39 -
4. 3. 1 Characteristics of the ISO Standards - 39 -
4. 3. 2 Analysis of ISO 9001 / 27001 - 41 -
4. 3. 3 Interim Summary of ISO Standard Features - 43 -
4. 4 IT-Grundschutz by BSI - 44 -
4. 4. 1 Characteristics of IT-Grundschutz - 44 -
4. 4. 2 Analysis of IT-Grundschutz - 46 -
4. 4. 3 Interim Summary of IT-Grundschutz - 48 -
4. 5 Analysis: Comparison and Contrast - 49 -
5 Model Collection QISMO - 51 -
5. 1 Integrated Framework of QISMO - 51 -
5. 1. 1 Representation of the Framework - 51 -
5. 1. 2 Specific Parts of the Framework - 52 -
5. 2 Reference Process of QISMO - 53 -
5. 2. 1 Model of the Reference Process - 53 -
5. 2. 2 Elements of the Reference Process - 55 -
5. 3 Lifecycle of QISMO - 58 -
5. 3. 1 Model of Continuous Management - 58 -
5. 3. 2 Elements of the Lifecycle - 59 -

6 Validation of the QISMO Models ..... - 61 -
6. 1 Evaluation by Criteria ..... - 61 -
6. 1. 1 Evaluation of QISMO Models by Criteria ..... - 61 -
6. 1. 2 Summary of Model Evaluation by Criteria ..... - 63 -
6. 2 Evaluation by Experts ..... - 64 -
6. 2. 1 Conduct of Model Evaluation by Experts ..... - 64 -
6. 2. 2 Summary of Model Evaluation by Experts ..... - 65 -
7 Discussion ..... - 67 -
7. 1 Appraisal of the Approach ..... - 67 -
7. 2 Results of the Study ..... - 69 -
7. 3 Directions for Further Research ..... - 73 -
8 Conclusion ..... - 75 -
Publication Bibliography ..... - 77 -

List of Figures

Figure 1: Sectors of Critical Infrastructure ..... - 3 -
Figure 2: PDSA-Cycle adapted from Deming (1993, p. 135) ..... - 10 -
Figure 3: The Socio-Technical Information System (own figure) ..... - 12 -
Figure 4: Adapted Model for the Applied Research Methods and Process (own figure) ..... - 27 -
Figure 5: COBIT Principles. Source: ISACA, COBIT 5 2012, p. 13 ..... - 32 -
Figure 6: ITIL® Lifecycle, adapted from OGC (2007, p. 19) ..... - 35 -
Figure 7: Elements of a single process. Source: ISO 9001:2015, p. viii ..... - 39 -
Figure 8: Phases of the BSI Security Process. Source: BSI, 2008b, p. 12 .. - 44 -
Figure 9: Framework for Quality and Information Security Management for small Organisations (QISMO) ..... - 51 -
Figure 10: Reference Process for the Simultaneous Development of Quality and Information Security ..... - 54 -
Figure 11: Lifecycle of QISMO ..... - 58 -

List of Tables

Table 1: Number of Companies by their Size in Germany 2013 (DESTATIS, 2015b; 2015a) ..... - 3 -
Table 2: Process Modelling Rules. Source: Mendling et al. 2010, p. 130. .. - 25 -
Table 3: BPMN Basic Modelling Symbols ..... - 28 -
Table 4: COBIT 5 Summary by Evaluation Criteria ..... - 34 -
Table 5: ITIL v.3 Summary by Evaluation Criteria ..... - 38 -
Table 6: ISO 9001 and ISO 27001 Summary by Evaluation Criteria ..... - 43 -
Table 7: IT-Grundschutz Summary by Evaluation Criteria ..... - 48 -
Table 8: Concluded Disadvantages of Standards and Good Practices ..... - 49 -
Table 9: Elements of the Reference Process Model ..... - 55 -
Table 10: QISMO Summary by Evaluation Criteria ..... - 63 -
Table 11: Summary of the Evaluation by Experts ..... - 66 -
Table 12: Alignment of the Research with the Findings of the Study ..... - 68 -
Table 13: Comparison of the Approaches ..... - 71 -

List of Abbreviations

APT	Advanced Persistent Threats
BISE	Business and Information Systems Engineering
BMWi	Bundesministerium für Wirtschaft und Technologie
BPMN	Business Process Modelling Notation
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
COBIT	Control Objectives for Information and Related Technologies
CPS	Cyber Physical Systems
DDoS	Distributed Denial of Service
GOM	Generally Accepted Modelling Principles
GOM II	New Generally Accepted Modelling Principles
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ISR	Information Systems Research
ITGI	IT Governance Institute
ITIL	IT Infrastructure Library
KPI	Key Performance Indicators
MSE	Micro and Small Enterprises
OECD	Organisation for Economic Co-operation and Development
OGC	Office of Government Commerce
PDSA	Plan-Do-Study-Act
SLA	Service Level Agreement
QISM	Quality *and* Information Security Management
QISMO	Quality *and* Information Security Management for Small Organisations
QMS	Quality Managements System
SME	Small and Medium Sized Enterprises
WKWI	Wissenschaftliche Kommission Wirtschaftsinformatik

Abstract

This master thesis elaborates the construction of an integrated framework for the simultaneous initiation of quality management *and* information security management within micro and small enterprises. Called QISMO, the model collection consists of three parts: (1) a holistic framework as structure dedicated to achieving a shared understanding among key stakeholders concerned about relations and dependencies, (2) a reference process model for visualising the entire process with the activities related, and (3) a lifecycle model for illustrating the process loop and for clarifying specific phases therein. This study offers an analysis of alternative approaches that results in premises and requirements adapted to micro and small enterprises. Furthermore, major barriers to the improvement of quality and information security management of micro and small enterprises are identified in this study. These include miscalculation of risks, lack of competence, and absence of structured processes. Aside from valuable insights for further development of enhanced training programs, the study contributes a comprehensive analysis of standards and good practices within the field of IT governance. Moreover, the study shares a concrete reference process model that is adapted to the preconditions of micro and small enterprises. These preconditions are acquired throughout the study. The proposition is to provide a basis for the further improvement of business processes and the models related to them, both in practice and in research.

Keywords: Quality Management, Information Security Management, Information Systems Modelling, Reference Process Modelling, BISE, BPMN

This page has been intentionally left blank.

1 Introduction

This chapter discusses the rationale for and scope of this study. It also presents the problem situation of small enterprises in Germany and considers the main research questions and related work. An overview of the thesis structure concludes this introductory chapter.

1. 1 Motivation

Information security within IT governance is now frequently discussed in news media and scholarly journals. It is also considered in the context of company development strategies. The issue became more prominent after a few recent incidents: namely, the cyber-attacks on *TV Monde*[1] in April of 2015 and the attack against the *German Federal Parliament*[2], which received much media coverage for a long period of time. While the issue underlying this study has its roots in the current situation in Germany, the characteristics outlined below can easily be extended to other situations within Europe or worldwide.

The application of new technologies and devices—such as cyber physical systems (CPS) and mobile devices—creates a more complex situation for setting an appropriate level of information security within companies and organisations (Dong, Han, Guo, & Xie, 2015). This is particularly the case if these newer devices are not yet included in the process landscape of the quality management system (QMS) and if it is also possible that such a system has not yet been implemented within the organization. Several factors often lead to capitulation due to the complexity of the task; these factors include rapid changes, budget constraints, a lack of competence within an organisation, ignorance, and a dangerous lack of interest and capability among decision makers (Mishra, Caputo, Leone, Kohun, & Draus, 2014, p. 142). In addition, there are a number of strong barriers to organisational learning: namely, the fear of costs, the feeling of being at the mercy of attackers, and the fear of showing signs of weakness and weak points in the system. At the same time, the feeling of fear is necessary if changes are to take place within an enterprise (Liebmann & Kraigher-Krainer, 2003, p. 5).

[1] https://twitter.com/TV5MONDE

[2] http://www.n-tv.de/politik/Beispielloser-Angriff-auf-den-Bundestag-article15105711.html

Fear can easily force business owners to pretend that threats to quality or information do not exist. Rather than finding appropriate measures to tackle each situation within a reasonable budget, companies in general tend to act as if the problem is someone else's—in particular, that it is a problem of other, much larger organisations (Bourne, 2014). Furthermore, organisations often place much trust in technical and software solutions, but they may neglect or disregard the management of the processes and the human component of the socio-technical information system and the protection of the technical machinery against physical destruction (ATKearney, 2012).

To break down these barriers, awareness and sensitization campaigns have been carried out by different government ministries, such as the Federal Office for Information Security in Germany and the Local Chamber (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2011, p. 42). However, most changes take time, and the process of change can be a slow one both for larger and smaller companies. Only after an incident is detected, problem-solving activity accrues. Without proper process structures and documentation, rational inventory and problem hunting within an adequate timeframe seem to be nearly impossible. In particular, micro- and small-sized enterprises (MSE) in Germany currently face a challenge in managing such problem situations because they often lack quality management and information security management systems (BSI, 2011, p. 9). In addition, such enterprises are confronted with personnel and experience constraints due to their size and budget (Bundesministerium für Wirtschaft und Technologie (BMWi), 2012, p. 9).

1.2 Problem Description

The aforementioned issues bring a stronger focus on information security, particularly in critical infrastructures in Germany. Due to increased dependence on electronic devices, the Internet, and requirements of privacy, the IT-Security Law (IT-Sicherheitsgesetz) was established in Germany on 25 July, 2015. At present, the concrete requirements for the implementation of the law are still under development. This requires more and adequate actions from organisations that run critical infrastructure. The security level has to be tested and documented by an independent auditor to ensure that it is at an acceptable level. Operators in the sectors of telecommunication and website hosting are affected first, followed by those in the sectors of water, food, and energy and nuclear substances.

The last group affected includes branches such as transport, traffic, finance and health. As illustrated in Figure 1, many larger organisations within these sectors of critical infrastructure—e.g., German hospitals[3]—are already legally forced to maintain a quality management that is attested by external audit for many years.

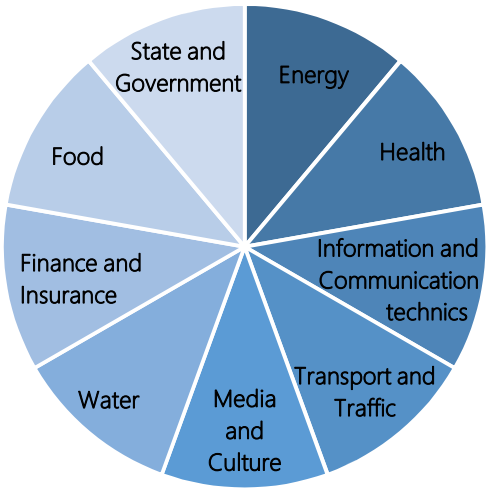


Figure 1: Sectors of Critical Infrastructure

Many of the organizations currently impacted are larger companies that have a reasonable process of IT governance in place that includes the auditing of implemented processes, methods and measures. However, many organizations are MSE. As an example, Table 1 shows the structure of companies by size of the enterprise in Germany in the fiscal year of 2013. The structure among companies within the European Union (Eurostat, 2015) looks fairly equal.

Table 1: Number of Companies by their Size in Germany 2013 (DESTATIS, 2015b; 2015a)

Total	Micro < 1 Million Sales in €	Micro/ Small 1 to 2 Million Sales in €	Small 2 to 10 Million Sales in €	Medium 10 to 50 Million Sales in €	Large > 50 Million Sales in €
3.629.666	3.267.113	156.021	154.073	40.171	12.288
Employees	Up to 9	Up to 9/ 10 to 49	10 to 49	50 to 249	> 249

Small and medium-sized enterprises (SME) constitute the larger part of the providers in the above-mentioned critical infrastructure. For instance, in the energy sector, only 192 out of 61.969 firms are larger firms in Germany. A similar situation can be seen among providers of information and communication (434 out of 130.027) and healthcare, where 234.710 out of 236.900 are SME (DESTATIS, 2015a).

[3] § 135a SGB; https://www.jurion.de/Gesetze/SGB_V/135a

Sensitive personal data is typically handled and processed in these branches within critical infrastructure, as Figure 1 shows. It can be seen that the maintenance of their functionality has an important impact on society. The providers of healthcare are particularly committed to detailed documentation concerning patients and their individual treatment. Likewise, the requirements for this documentation have been tightened within the telecommunication, transport, and traffic sectors. The data that is collected in all these sectors creates a large set of data to process, protect and preserve.

Smaller businesses focus on core business during day-to-day activities, especially in their beginning stages. When a company grows quickly, its owners may lose track of activities. A QMS adapted to smaller organisations can help to keep the focus on customers and avoid mistakes, particularly recurring ones. Besides the advantages of a QMS—such as a higher transparency around processes within a company and a better quality of products—smaller companies may experience some disadvantages, such as difficulties with the documentation of existing processes and a lack of acceptance from employees (RKW, 2008, p. 12). Although technical premises within small enterprises are often quite good, there are deficits in documentation of business processes and IT security management, and these deficits have been neglected (BSI, 2011, p. 9). Frequently, management of information security is either not done or not adequately structured (Jonsson & Wehrmann, 2015, p. 34). This point raises the need for the development of an adequate framework for quality *and* information security management (QISM) as well as a reference process model related to the QISM and adapted to the demands of MSE.

Although there are many standards and good practices available for purchase or for free, 73% of organizations rate threats to information security as increasing, and around 78% of organisations see a need to improve their security measures (BSI, 2014, p. 12, 17). More than half of organizations know that they have been victims of a cyber-attack. Because Germany ranks high in the number of cyber-attacks (Kim, Wang, & Ullrich, 2012, p. 68), it is conceivable that the estimated number of cases remaining undetected is considerably higher. This shows the extent of the flaw in the management processes within organisations regarding personal data and internal business data, both of which are necessary to the maintenance of operability and competitiveness and for privacy concerns and civil protection.

1. 3 Research Question and Contribution

The scientific discipline of *Wirtschaftsinformatik*—also known as business and information systems engineering (BISE)—establishes the interdisciplinary bridge between business administration and information systems. Particular attention is given to the socio-technical system and its development within companies and organisations. The design and further development of concepts, methods and information systems—and the investigation of value-creation processes and relating human/employee behaviour—are core aspects in the broad research area (WKWI 2011). This thesis focuses on the management and governance part of the socio-technical information system.

This study examines the comprehensive research field of business and information systems considered from the perspective of MSE in Germany. It is done within the contexts of IT governance, quality management, information security management and reference process models associated with that field. The particular preconditions and limitations are also considered. In relation to the above, the following research question is formulated:

- *How can an integrated framework and a reference process model be created to simultaneously initiate quality management **and** information security management in MSE?*

To elaborate an answer relevant to the main research question, the following sub-questions are also investigated:

- *What are the major barriers for MSE in the case of the preparation and implementation of an appropriate level of information security?*
- *How can these obstacles be affected to overcome them?*
- *What standards and good practices exist, and what distinctions and possible deficiencies can be identified?*
- *Which elements contain an appropriate reference process model?*
- *What recommendations for action can be derived from the survey?*

This thesis contributes to the structuralisation of the problem situation regarding quality management and information security for MSE, particularly in Germany, with the hope that the results might be applicable to the rest of the European Union in the near future, especially if other states also establish an IT security law.

This study focuses on the development of an integrated framework and the referential management processes corresponding to the structure of the framework. The term *framework* is used throughout the study along with the defining meaning of a conceptual framing to a specified problem. The models constructed are dedicated to the simultaneous establishment of an appropriate level of quality and information security in MSE. This could also constitute the appropriate ground for a certification of individual corporations.

The research in this study mainly aims to achieve a threefold contribution to the stated problem of improving organisational information security and attaining adequate quality management within the context of small organisations.

First, barriers to improvement are investigated throughout the following survey in order to derive adequate strategies for further development from the examination and the models. In this way, valuable insights for the further elaboration of guidelines and training programs can be obtained.

Second, this study aims to build an integrated framework using insights gained from a comprehensive analysis of existing standards and methods in the field of IT governance, including quality management and information security management as a base. This is done to achieve a shared point of view on the subject.

The final objective of this study is to construct a reference process model for the easier implementation of an appropriate quality and information security management system within small enterprises. The goal is to contribute to an enhanced standard of quality and information security among smaller organisations.

To answer the research questions, the study starts with a review of relevant literature within the fields to find quantitative analyses and qualitative phenomena, such as behavioural studies and conceptual foundations. These are used to offer the necessary background to the topic. Furthermore, the study is based on and dissociated from other works related to the subject, as the following section demonstrates. Chapter 3 establishes the specification of the research methodology applied within this paper.

The concepts in this study are aligned with the approach to design research proposed by Hevner (2007; et al. 2004). They follow the cognitive process of the design-oriented information systems research applied in business and information systems engineering by Österle et al. (2011).

This thesis is addressed to two main audiences: namely, professionals and scholars within the research fields concerned who focus on similar aspects, and individuals who are responsible for quality management and information security management within small enterprises and organisations.

1. 4 Related Work

A number of studies have been conducted regarding information security in the context of small organizations. A comprehensive literature review and analysis has been published on how well the needs of small businesses are answered by the International Organisation for Standardisation's (ISO) 27001 standard. This review identifies barriers to adoption and encourages further research in the origination of, "simplified security methods or standards [...] in order to create a framework of certification dedicated to SMEs" (Barlette & Fomin, 2008).

A survey commissioned by the BSI compares selected standards and good practices. This provides synergy effects, which can be gained in the combining of standards during implementation. The survey takes a rather general perspective and focuses not solely on the specific needs of SME. (BSI, 2009, p. 48)

Previously, the conjunction of business approaches with a process focus has been suggested for the benefit of improving the management of information security within organisations. Although this holistic approach has strong potential to integrate different methods of security risk management within a company at a strategic level, it lacks procedure models and guidelines for practical implementation specifically tailored to smaller businesses. (Sowa, Tsinas, Lenz, & Gabriel, 2009, pp. 334–336)

A structural model for organizational information security has been designed by Reeg (2011). This model illustrates relations between aspects of information security to a socio-technical system and has been used to evaluate existing concepts of information security. The conceptual approach provides a method for the development of security-enhanced business-process models. (Reeg, 2011, p. 146)

Baseline safeguards tailored to SME are discussed to add easier and better security facilities to consumer devices and to SME themselves; these safeguards can consistently provide a higher level of security even through the supply chain

(Clarke, 2015, p. 541). Nevertheless, they offer no procedural support for the implementation of information security safeguards to SME at the starting point.

1. 5 Structure of the Thesis

This study is structured as follows. Chapter 2 establishes elementary foundations within the management of information systems in general with a particular focus on quality management and information security in small enterprises. The basics in modelling are also presented in this chapter. Chapter 3 illustrates the research process applied in the study. It also contains a short introduction to the discussion within the research area and to the research method spectrum adapted to the current research. The modelling process that is conducted is also illustrated in more detail in this chapter. Chapter 4 describes and analyses existing standards and good practises in accord with the evaluation criteria discussed in section 3. 3. 3. Following this, Chapter 5 develops an integrated framework that provides holistic structure to the problem situation. It represents the situation of key stakeholders concerned as well as dependencies to information and business processes within MSE in Germany. Moreover, the chapter constructs and characterizes a reference process model and a lifecycle model. The latter aims to increase understanding of the continuality of the approach, and it completes the model family presented in the chapter. Chapter 6 evaluates the model family that is constructed with an application of the aforementioned evaluation criteria and an investigation by experts. Chapter 7 discusses the results and the approach along with other possible research needs. Finally, the conclusion in Chapter 8 summarizes the research process and provides answers to the research questions; it also rounds out the thesis with a consideration of possible further research issues.

This Chapter introduced the work in the area of IT governance, particularly the aspects of quality management and information security management within the context of MSE. Furthermore, studies previously performed were highlighted. After providing a deeper insight into the problem area and the research questions in this chapter, Chapter 2 provides the background to the specifics of the problem situation for smaller organisations.

2 Foundation

This Chapter presents background to the scope of the current research paper within information systems management in general and information security in SME in particular. Furthermore, it describes the theoretical and practical features of modelling with a particular focus on reference process modelling.

2. 1 Management of Information Systems

2. 1. 1 Corporate & IT Governance

Enterprises are market-economy-oriented business entities that follow the principle of profitability (Gutenberg, 1983, pp. 458–459). This profitability rests on two pillars: functionality and conservation of resources. To manage these in daily business activities, management strategies and controlling activities are subsumed under *corporate governance*. This term is defined as follows:

> "*Corporate governance is one key element in improving economic efficiency and growth as well as enhancing investor confidence. Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders.*" (OECD, 2004, p. 11)

Management activities include arrangements for external and internal relationships regarding the achievement of a company's objectives, and compliance with legal regulations and customer requirements. Information technologies in all their facets have achieved ubiquitous penetration into the routine of business, both in larger and smaller enterprises. This penetration has grown to such a degree that even IT governance—following the parameters given by corporate governance—has become an important part of organisational management. Owing to this, IT governance has to support the accomplishment of profit and growth for a company. On the other hand, it also needs to reduce IT-related risks to protect its value and resources (Johannsen & Goeken, 2007, p. 21).

To support the implementation and maintenance of IT governance within the enterprise, various standards and good practices have been elaborated. Some of these are concerned with strategy development at a theoretical level: e.g., the strategic alignment model (SAM) used to align businesses with the IT strategy (Henderson & Venkatraman, 1999, p. 476). Others focus on management

processes related to IT in a company. From these existing good practices and standards, several approaches are chosen for further analysis in Chapter 4. These include one with focal point on IT governance (COBIT), one on IT service management (ITIL), one on quality management (ISO 9001) and two focussing on information-security management (ISO 27001 and IT-Grundschutz).

2. 1. 2 Quality Management

Since the early 1900s, there has been ongoing inspection of industrial production output with the purpose of sorting out faulty goods, and this process has undergone vast changes up to the present stage of quality management. This has changed the focus from producing better products and industry processes to meeting specific customer needs and to the continuous improvement of all business processes and decisions within a company.

The Plan-Do-Study-Act (PDSA) Cycle, significantly developed by *Deming* (1986, p. 88)[4], is one of the most consulted and applied. The cycle as a loop emphasizes the continuous rotation of the four steps with quality as the aim. The approach and its steps are represented in Figure 2.

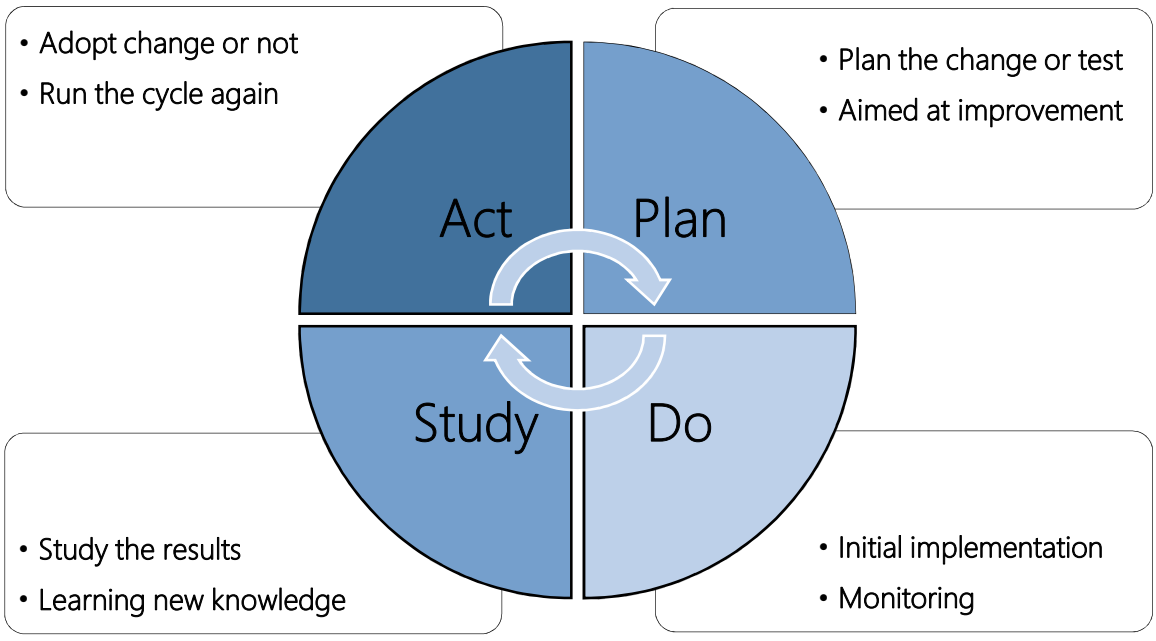


Figure 2: PDSA-Cycle adapted from Deming (1993, p. 135)

[4] Regarding the changes during the history of the PDSA see: Moen, R., & Norman, C. (2009). The History of the PDCA Cycle. In *Proceedings of the 7th ANQ Congress Tokyo 2009, September 17, 2009.*

Planning is the starting point of all activities. Several actions are performed in this step: the situation is analysed, the potential for improvement is examined, and the general conditions are defined. Next, promising alternatives are initially implemented and monitored. In the next step, results from the previous phase are studied. Implications for the project have to be considered and conclusions discussed. In the final step, responsible individuals decide whether changes will be implemented and what their concrete implementation will be.

The third step of *study* is particularly important to the improvement of the quality of the product, service or process. Within this step, the activities concentrate on learning from failure and success, through which new knowledge can be constructed. It is believed that only new knowledge brings improvement.

Running the structured approach continuously can help to maintain a constant level of quality for a subject of the loop. This fact itself gives no evidence about the certain level of quality, which means that the quality itself does not necessarily need to be *good*. In other words, the willingness to improve and learn is crucial to the success of quality management. Thus, quality management is not a substitute for proper management; quality is the responsibility of the management of a firm and should be in its particular interest.

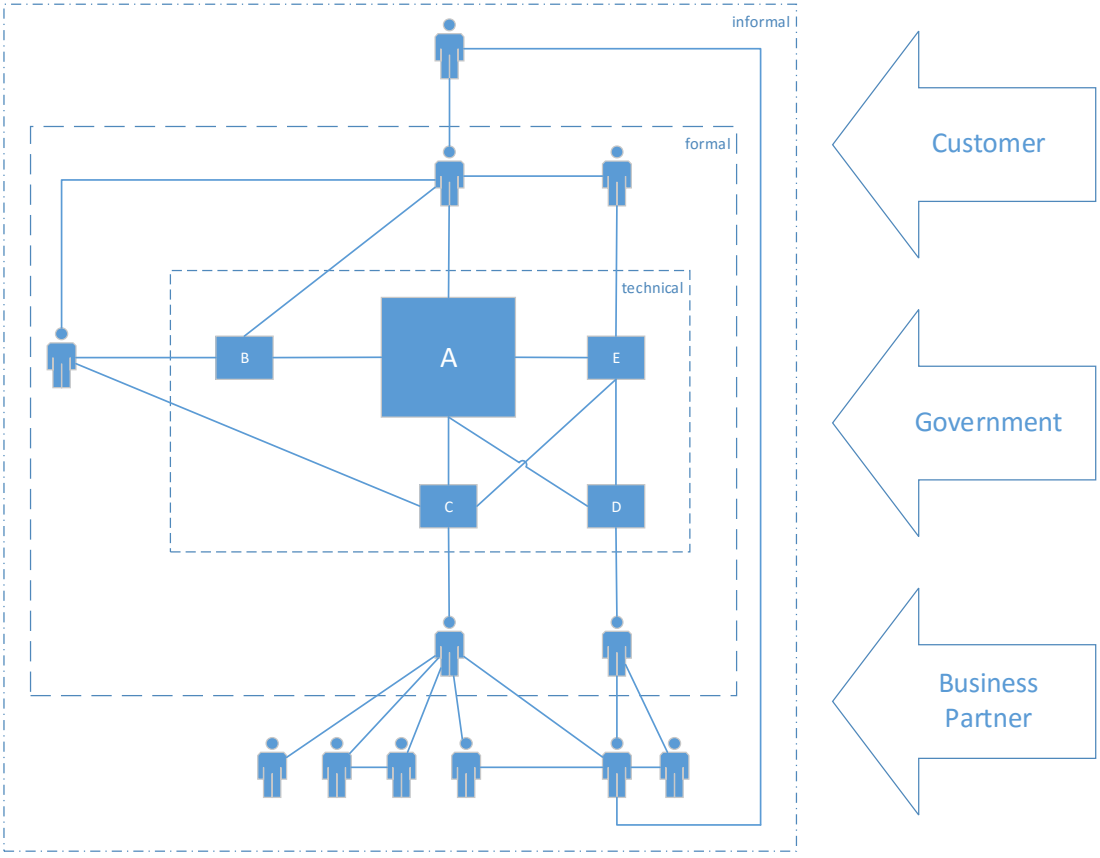
The cycle above also involves constant documentation of actions and responsibilities as well as the monitoring and evaluation of any measurements. This documentation provides the basis for learning and improvement, both for larger organisations and smaller companies (Bayerisches Staatsministerium für Wirtschaft und Medien, Energie und Technologie, 2012, p. 22, 26). Moreover, it can be used for an external audit for the purpose of obtaining an independent certification according to approved standards; this is done to meet the requirements from customers or legal regulations. International standards are only partly implemented in MSE and SME. More effort is necessary for smaller organisations to place themselves in a better market position in the international context (Aziri, 2015).

2. 1. 3 Information Security Management

As a part of IT governance, information security (ITGI, 2006, p. 45) has the function to ensure the protection of information resources within the organisation. This requires that threats are identified and that countermeasures are established. In the course of the continual maintenance and development of information

security, it is necessary to have a holistic view of the socio-technical system and continuous management and improvement, including an organisational value system (Mumford, 2006, p. 338). Thereby, information security should be an enabler of organisational business and not a hurdle. The protection of information is critical to many organisations today. Information is handled in day-by-day activities within and outside the organization; in particular, it flows through the technical, formal and informal part of the socio-technical information system (Emery & Trist, 1960, p. 86). As a result, a holistic coordination and observation of the special challenges of the interrelated parts is requested (Bertalanffy, 1968).

Figure 3: The Socio-Technical Information System (own figure)



The technical part includes everything concerned with hardware, software and data protection, both physically and virtually. It automates a part of the formal system, which consists of all regularities and structures made to ensure security and integrity within the organization. The informal part of the system embeds the technical and formal. The complexity of information system security increases with different social groups within organizations and the information flow between organizations (Boulding, 1956, pp. 202–205; Kearney & Kruger, 2016).

Moreover, the system meets specific requirements from government, customers, and business partners. Figure 3 illustrates the system, its parts, and outside influences.

The management of a complex and dynamic information system involves having both appropriate control systems for the specific parts and an integrated management system that provide a holistic assessment of the current situation. Although organisations in general are aware of the need for an information security management system (ISMS), less than half of them have one already implemented. Major concepts in use include IT-Grundschutz and ISO 27001. Only a fraction of those have been certificated through an external audit (BSI, 2015, p. 29).

Social and technical aspects of ISMS for larger organisations are transferrable to smaller organisations. Although differences occur due to the scale of the system, the threads are similar. This will be discussed in more detail in upcoming sections. Because threats are similar to organisations regardless of their size, and because ISMS have not been implemented reasonably (BSI, 2011, p. 42; Clarke, 2015), the government has placed higher requirements by regulation. The new legal requirements in Germany demand better and more appropriate measures along with the implementation of a documented management process to allow an external audit from many, even smaller, organisations.

2. 2 Information Security in MSE

2. 2. 1 Threats to Information Security

There are various threats to information security, and their potency depends on multiple factors. These include the uncritical use of diverse devices, unsecure Internet connections, and the unintended exposure of secret information by a common user. Furthermore, technical issues such as outdated software or industrial control systems that are inadequately hardened can open the door for attacks. The ubiquitous use of all kinds of *connected things* adds a habit of digital carelessness that can be easily and dangerously exploited by an attacker who is interested.

Typical attacks include spam—commonly spread by email—and malware. Other common attacks include software exploits, distributed denial of service (DDoS), theft of identity or information, advanced persistent threats (APT) for misuse of systems and social engineering.

Some organisations admit to having been targets of a successful attack to their information security; they have indicated that a large number of attacks are random malware infection by drive-by or email-spam (BSI, 2015, p. 13). DDoS-attacks on websites are the second most common attack. Targeted malware infection by social engineering or USB-devices, hacking-attacks in order to misuse systems or websites, and DDoS-attacks on network infrastructures lie nearly on the same level among noticed attacks (ib.). The attacks are believed to be linked to the unwitting misbehaviour of employees, zero-day exploits, and unpatched and misconfigured systems. Only 17% of the known attacks are traced back to social engineering and 8% to intentional insider attacks (ib.). This raises questions about whether all attacks of these two kinds could have been detected.

Although threats from malicious insiders are small in comparison, data spillage and insecurity of information caused by a non-malicious insider can result in an enormous attack-vector that needs to be considered within company culture and organisational policies (Wall, 2012, p. 122). Social engineering that attempt to get unauthorized access to information is as old as the existence of groups of individuals with different levels of information and authority. Different methods are used to obtain information, and the attacker may not always be aware of the inappropriateness of his activities. When reprisal is a reality, unauthorized access can be given as a result. Even social media can be used to share information to garner appreciation. Such relations between individuals with an unhealthy imbalance can be hard to detect and can become difficult to leave. This threat to privacy and information security remains in force due to human nature, and there needs to be enough consideration in organisations by education and policy documents (Thornburgh, 2004, p. 135).

In order to compound the hazardous situation, the application of unsecure devices and a misperception of threats within an organisation are related to the characteristics of the decision maker. Limited experience leads to a lower estimation of potential risks and weak points in a complex socio-technical system, and wrong decisions for appropriate measures can be made as a result (Grant, Edgar, Sukumar, & Meyer, 2014, p. 108). Moreover, smaller companies often use standard products and software due to the costs. Unsecure developed components can be difficult to detect in the system if management does not have sufficient relevant knowledge.

This is why those who consider in-built security features and independent test results of used components and devices should appeal to SME if they wish to overcome market failures (Clarke, 2015, p. 547).

Since SME represents a large portion of all enterprises, a problem situation of threat can affect both company success and public safety; this can be caused by a combination of very low deployment of resources dedicated to organisational information security and by the estimation of increasing attacks on it.

2. 2. 2 Impact of the Violation of Secrecy

The impact of obtaining unauthorised access to information can vary. There may be no impact—mostly because it goes unnoticed—and it may result in small consequences such as a penalty or a formal apology, or there may be huge consequences for a company's reputation that can threaten economic survival even for the environment and society. Although the concerns of avoiding big issues depend on the underlying vision of the respective organisation, the economic aspect is equally important to all organizations. In general, organisations view disturbances or interruptions to their daily business as the cause of damage at the greatest level. In addition, the costs for a clearance of the incident and the recovery of operability are estimated to be so high that an improvement of the appropriate measures is deemed necessary (BSI, 2015, p. 17, 28). Even though short-term planning of costs is elementary to companies, long-term effects have to be considered too.

The relation that an organization has with its customers is particularly important. There are important factors that an organization needs to build trust. One is privacy: the offered and expected protection and control of an individual's private information (Nofer, Hinz, Muntermann, & Roßnagel, 2014, p. 341). Another is security: new customers appear to be drawn to companies that have adequate security, which means the actual measures and its effectiveness for the secure storage of data (ib.).

Customers who become more knowledgeable and informed regarding privacy or security incidents tend to spend less money on the products of the company (Nofer et al., 2014, p. 344). This immediately suggests that violations to information security can have enormous consequences for companies, especially if these violations are subject to medial interest. Negative publicity—which may be caused

or intensified by the ubiquitous use of social media—can result in a wide spread with the aforementioned consequences.

Even though threats from malicious insiders are not that common, they are far from new (Fox, 2003), and the damage that can be done to an organisation would require both education and management to follow. Control measures and policies help to reduce the impact of this problem on relevant company goals. These are economics, represented by short-term costs, and company reputation represented by long-term customer relations. Both goals are elementary to the survival of the entire enterprise.

Furthermore, another dimension can be added if the possible influence on both the environment and society is contemplated. Regarding critical infrastructure in particular, the effects of an information security breach have the potential to cause severe damage to the environment, which can result in severe complications of the circumstances of survival and even in terror. As a result of globalisation, local problems can rapidly grow into a global issue.

2. 2. 3 Barriers to Enhanced Information Security

Given commonly known threats and the conceivable impact of information security breaches, the main barriers to the implementation of an appropriate level of organisational information security needs to be uncovered.

First, the miscalculation of risks and the misjudgement of one's own ability to action can be distinguished. This point refers to making management decisions to specify an appropriate level of security—such as the type of security and the extent of the measures that need to be taken—and to assess the efficiency of the chosen solution. In addition, the quantification of the cost and benefits of the measures by a structured approach in SME is often substituted by inconsistent distinct estimations, which show an inadequate experience level and general human misjudgement. Since short-term costs are overestimated and are weighted higher than long-term benefits (Jonsson & Wehrmann, 2015, p. 33), there may be a situation in which either the required decisions or the appropriate measures are delayed until an event occurs that forces immediate action.

Second, the aforementioned barrier goes along with the deficiencies in awareness training and education. Many employees report that the measures for improving

the information security could hinder efficient work flow. They can be excessive due to miscalculation and inappropriate due to the misinterpretation of the importance of behaviour (Fox, 2003, p. 677). Furthermore, small organizations commonly have only one employee, if any, who is responsible for information security. This employee is usually the only person who oversees the entire technical infrastructure and often does not have an appropriate competence in security standards. Apart from this, many small organisations lack proper experience (Jonsson & Wehrmann, 2015, p. 33), interest in the topic, time and practical training (Heier & Garret, 2015, p. 41).

Third, there may be an absence of structured processes, routines, properly customized policies and audits of the measures. Since the outcome of the firm is an important aspect of an organisation's daily business, costs and employee time can be scarce. According to these constraints, process documentation, policy development and management activities are generally reduced to the absolute minimum in SME. Usually, smaller businesses have grown without adjusting their business structure. This implies that responsibilities are not specified clearly. In combination with a heterogeneous, wild-grown IT landscape that is mostly undocumented, the work required to shape a structured and integrated management system seems time-consuming, and benefits are not easily recognized at this stage. Consequently, the business stays in a state of inefficiency until the head of the firm either acts as a good example for information security (Heitmann, 2007, p. 84) or adequate actions are required by law as statutory requirements or by business partners and customers. It is also possible for both to take place.

Lastly, SME lack organisational measures even if the implementation of technical measures such as firewalls, antivirus software, password authentication, backups and patches are in place and well realized (BMWi, 2012, pp. 25–26).

2. 3 Modelling

2. 3. 1 Model Features

QISM from initial planning via implementation and maintenance to the process of change and continuous improvement is characterized by its many and varied decision processes and complexity. Several considerations are necessary to master the complexity of the task. Aside from the usage of convenient methods and tools,

it is vital to shape a more in-depth understanding of the relationships of cause and effect of the participating factors. Model construction is one option that can be used to support this shared understanding. The essential characteristics of a model are presented by *STACHOWIAK* (1973, pp. 131–133):

- **Mapping**: This aspect refers to the perceptible correspondence between the original and the model. The modeller maps a selected segment of the original with a specific intention. This already implies a subjective abstraction by the modeller within its individual-cognitive model.

- **Reduction**: This feature signifies a goal-oriented, objective abstraction as the central characteristic of a model. This feature aims to reduce the complexity of the real world situation by omitting irrelevant details and by emphasizing the relevant details. A principal motivation for reduction lies in the intention to have minimal effort for both the model construction by the modeller and the model processing by the target audience. During model construction, it is important to consider the perspective of the target audience and the audience's ability to handle and interpret the model. Based on the competence of the observer, an individual-cognitive model will be formed from the observer's view. This can be the same or other than the modeller initially had in mind.

- **Pragmatism**: This point characterizes the requirement of a certain chronological and expedient placement of the concrete model. An accidentally occurring image is not a model. A model is characterized by its intended purpose and chronological integration directed at a concrete user.

Another classification of models can be formed from the method used for mapping. Models can be of the following types:

- **Sign based**: This encompasses models that deploy verbal means to determine the model elements such as program code, mathematics, and even native-language descriptions.

- **Graphical**: This kind of model comprises pictorial constructions and structures. It can also contain sign-based details, such as sketches and diagrams.

- **Technical**: This group of models includes models without limitation, tangible models, three-dimensional models such as physical prototypes and electro-technical models.

Due to the immateriality of management processes, sign-based and graphical models are usually used to conceive, control and develop business processes. The modelling of physical samples is not discussed in this study. Different methods and approaches exist for two-dimensional model construction of sign-based and graphical models. The specific procedure applied and adapted to the current research is outlined in section 3. 3.

2. 3. 2 Model Building

Depending on the purpose and the intended target group of the model, reducing the complexity of the actual or imagined reality by target-aimed abstraction is fundamental. The process of the development of a usable model can require several increments of abstraction if the complexity of the concrete model is beyond the boundaries of the respective model constructor and its tools. (Grochla, 1974, p. 17)

To keep the complexity of a model manageable, a highly competent model constructor is required in addition to proper tools. Software-tool based support can be helpful for the construction task and the reuse of models as well as parts of models. In other words, modelling tools are preferred that control adherence to the syntax and semantics of the modelling language of the meta-model to enhance the quality of the models constructed.

Moreover, whether a defined modelling language or merely a graphical notation adapted for the purpose is used should be decided by the usability, availability and potential of a requirement-specific configuration. The purpose of the model and the competencies of the target audience anticipated by the modeller influence the selection of the mapping medium, methods and tools used for construction.

The level of accuracy of the model can be indicated in the following ways:

- **Informal**: Models at this level are originated by people in a creative way, and they cannot be automated using verbal descriptions or sketches. The interpretation of the model is not automatable because the model generation does not follow determined rules.

- **Semi-formal**: Semi-formal models are partly constructed by observing formal rules and even contain informal elements such as remarks in natural language. These models have to be interpreted by an individual observer.

- **Formal:** Models of this category are constructed with the support of a modelling language that defines formal rules in the form of syntax and semantics. Therefore, these models are easily automatable, but they are not error tolerant.

Models can be developed for various purposes with specific responsibilities, as described below:

- **Description function**: These models map the facts and circumstances of a case, and they create a basis for communication and a shared understanding. Process documentation has such a description function, for example.

- **Explanation**: These models represent the relations of cause and effect, and they support the segment of the original with reasons. Examples include models for analysis or planning.

- **Decision-making**: These models assist with improved decisions that assume optimisation objectives, such as statistical and mathematical models of operations research. This kind of model is used in simulations and prognoses of outcomes with modified variables.

Models build a significant basis for communication and the moulding of organisational information systems. Moreover, they are vitally important to the development of organisational procedures as well as quality and information security processes. Furthermore, they act as an interface between management, internal user, customer and auditor.

Based on the above discussion, this study uses the term *model* to describe a pictorial representation of conceptual or real world circumstances that is purposefully reduced to meet the specific perspective of an intended user.

2. 3. 3 Reference Model

There are different types of reference models: namely, procedure (or process) reference models, application-system reference models and organisation reference models (Schütte, 1998, p. 71). Reference models can be used to describe the common aspects of a class of models; they can even be used in a prescriptive manner as a suggestion for the elaboration of these models.

- **Procedure reference models** represent a kind of pattern for the description of a development state, and they also provide suggestions for achieving the objectives intended (Fischer, Biskup, & Müller-Luschnat, 1998, p. 18). This type of model is mainly used in the area of business process (re-) and software engineering in order to improve communication among key stakeholders involved and to shape requirements that are clearly defined.

- **Application system reference models** refer to typical functionalities and data structures of integrated standard software systems. They are intended for the visualisation of complex processes and applied as a basis for implementing process-oriented software systems (Reiter, 1999, pp. 49–51).

- **Organisation reference models** show organisation-specific models for company objectives. In this type of models, organisational structures for an intended purpose are related.

Aside from these types of reference models, a more general understanding of reference models includes the reuse of the elaborated models both intended and practical. This means that the model has either been constructed with the intention of reusability or that it has actually been reused (Vom Brocke, 2003, pp. 36–38).

With the above in mind, the definition used for this study combines the purpose of the reference model and its process orientation with the goal to facilitate both the reuse of the artefact and the efficient derivation of organisation-specific aspects as suggestions from the model that will be built.

Similarly, the reference models constructed serve to neither verify nor validate statements nor to explain facts. Rather, they are intended to map a larger range of real situations and to act as pre-build solution models or even as a general recipe for a class of decision problems that is used to master practical issues (Kosiol, 1964, p. 758).

This chapter described the foundations areas on which this study. Apart from elements of the management of quality and information security within information systems, barriers for enhanced information security in MSE were examined. Furthermore, the basics of modelling and reference process modelling were explained.

This page has been intentionally left blank.

3 Research Process

This chapter opens with a discussion of information systems research, which is followed by a description of the method spectrum applied to the study. The chapter also explains and clarifies aspects of the reference and process modelling approach as well as the evaluation criteria applied in this study.

3. 1 Information Systems Research

The research conception used in this paper is grounded in the pluralistic method spectrum of information systems research (ISR), which is particularly used in the BISE discipline in German-speaking research. It has been argued that a behavioural or hermeneutical approach that is strictly applied is often less than ideal in the context of ISR. A better contribution to the real-world problem and more useful research can be achieved when there is variety in applied research approaches and when research methods are configured to the individual subject of research (Frank, 2006, p. 62f).

14 core methods used in BISE appear in 300 research papers in the 1996–2006 period. These studies have been compared with methods used in ISR (original survey: Palvia et al. 2003) (Wilde & Hess, 2007, p. 285). A new study, conducted with similar premises, shows a constant application of the construction and design-oriented approach and a more mature method spectrum in papers recently published than that which appears in previous publications (Schreiner, Hess, & Benlian, 2015).

The debate on rigour *versus* relevance in ISR, as influenced by hypes and tendencies, illustrates challenges for the positioning of the related scientific research, particularly for the, "co-existence of fundamentally different research styles" (Winter, 2007, p. 403). In general, there is consensus on the importance of both *rigour* AND *relevance* in scientific research in the field. The appropriate methods are subject to change, and they are often a topic of discussions throughout the research community. The right balance of relevance and rigour depends as much on the subject and the target audience as on the state of the art in the research domain (Venable, 2007, p. 408). Knowledge transferred from academia to practice and vice versa should be considered both a very important part of academic research and an enrichment for both sides (Straub & Ang, 2011, pp. vii-viii).

The research approach applied in this study is aligned with design science research and its *7 guidelines* (Hevner, 2007; Hevner et al., 2004, p. 83); it follows the design-oriented process of *analysis, design, evaluation* and *diffusion* (Österle et al., 2011, p. 9). The methods used in this study with their components and the related *guidelines* are applied as outlined below.

3. 2 Applied Research Method Spectrum

3. 2. 1 Analysis – Standards and Good Practices

First, the analysis presented in Chapter 4 investigates existing standards and good practices regarding IT governance and QISM via literature review. In this section, common characteristics and differences between the relevant approaches are analysed and evaluated. They are then examined in relation to the situation of small businesses. For this purpose, the method of an argumentative-deductive analysis is used (Wilde & Hess, 2007, p. 284). Observations from the problem description (*Guideline 2: Problem Relevance)* can influence the analysis in an inductive manner (*Guideline 6: Design as a Search Process*).

To perform this analysis, the evaluation criteria are elaborated and adapted using the concepts of the foundation review as set out in Chapter 2; these criteria are formulated later in section 3. 3. 3. The application of the evaluation principles to the standards, which have been selected for analysis, can help to identify some advantages and disadvantages among the approaches investigated and thereby specify the requirements according to MSE for the reference model collection.

3. 2. 2 Design – Framework and Modelling

Second, from the results of the above-mentioned evaluation of existing approaches, an integrated framework is developed for the purpose of providing a holistic view on the specific situation in MSE. Developed via abstraction, the framework is presented on a conceptual level. It represents a generic model (*Guideline 1: Design as an Artifact; G6*). The main purpose of this integrated framework is to build a shared understanding of the problem issues related with the particular context and to contribute to further discussion and development in practice and in research (*Guideline 4: Research Contributions*). Furthermore, the framework provides a valuable strategic approach both for practitioners in enterprises and for researchers with similar interest. Moreover, a reference and a lifecycle model are

constructed for the purpose of preparing and implementing an appropriate level of QISM simultaneously in small businesses (*G1; G4*). As the core research approach in this part, methods of conceptual modelling are followed such as reference and process modelling from both inductive and deductive perspectives (*Guideline 5: Research Rigor*). For modelling of process models, *Mendling et al.* suggest some modelling rules as listed in Table 2.

Table 2: Process Modelling Rules. Source: Mendling et al. 2010, p.130.

Rules	*Meaning*
# 1	Use as few elements in the model as possible
# 2	Minimize the routing paths per element
# 3	Use one start and one end event
# 4	Model as structured as possible
# 5	Avoid OR routing elements
# 6	Use verb-object activity labels
# 7	Decompose a model with more than 50 elements

The authors have two aims in constructing these rules. First, they aim to provide better measurability of models constructed. Furthermore, they wish to enhance the modelling and analysis expertise of design engineers (Mendling, Reijers, & van der Aalst, W.M.P., 2010, p. 131).

Section 3. 3 outlines the core concepts and the modelling notation used in this paper in detail as well as the evaluation criteria. Moreover, the current study also examines the possibility of providing appropriate recommendations and guidelines for action within particular steps of the reference process model. This step completes the conceptual framework and reference process model with practical relevance and applicability (*G4*).

3. 2. 3 Evaluation and Contribution

Final, design results need to be evaluated. A significant number of methods are available (Hevner et al., 2004, p. 86; Pfeiffer & Niehaves, 2005, pp. 460–461). The artefacts that are constructed are evaluated and discussed in natural language using a plain-text and feature-based evaluation (Fettke & Loos, 2003, p. 83f) that follows the method *Descriptive by Informed Argument* (Hevner et al., 2004, p. 86). In other words, the argument for the utility of the model family is based on information from the knowledge base, which is used in conjunction with the

literature analysis (*Guideline 3: Design Evaluation*). The evaluation criteria used throughout the study are developed in section 3. 3. 3. Furthermore, a survey of several experts with relevant knowledge to the issue supports evaluation of the models. Finally, contributions to the knowledge gap and to the real-word problem, as described during the former Chapters, are explained and presented in the latter part (*Guideline 7: Communication of Research*).

3. 3 Reference and Process Modelling

3. 3. 1 Modelling Approach

For the most part, the construction process of the reference modelling used in this thesis follows the empirically grounded approach to the construction of reference models presented by *Ahlemann and Gastl* (2007). After the initial identification of a practical problem, this approach consists of five phases: (1) planning, (2) model construction, (3) validation, (4) practical testing, and (5) documentation (Ahlemann & Gastl, 2007, pp. 91–94). This process needs to be adjusted in some details according to the dimension of the present paper.

- ***Phase 1: Preparation.*** This phase includes all activities that are needed to prepare for the reference model. Within this phase, the problem scope is delimited, as in section 1. 2 (*G 2*). The methods are also defined, as outlined in Section 3. 2. Furthermore, the modelling characteristics and tools are specified as shown in sections 3. 3 (*G 5*). In addition to the process of *Ahleman and Gastl*, the results of the analysis performed in Chapter 4 reveal the required base of knowledge and data (*G 6*).
- ***Phase 2: Model Construction.*** This phase consists of the construction process of the framework, the reference process model and the lifecycle model. The construction is based on both the data pool collected in Phase 1 and the knowledge of the modeller (*G 1; G6*).
- ***Phase 3: Validation.*** In this phase, the model is evaluated (*G 3*). This study applies the evaluation criteria, as specified in section 3. 3. 3, to the constructed artefacts to identify advantages and disadvantages. Empirical validation is performed to a limited extent by way of a review by several experts.
- ***Phase 4: Practical Testing.*** Due to time constraints, this phase is omitted for this thesis. Since this phase can become very comprehensive if studied

elaborately, testing and refinement of the model can be part of a further survey or dissertation.

- ***Phase 5: Documentation.*** The documentation includes description of the modelling process, annotation and description of the model elements as well as complete documentation of data collection. To conduct this step properly, the documentation needs to follow the process and be entered in the finished thesis (*G4, G7*).

Figure 4 shows the adapted approach conducted in the research process in this paper. The methodology contains Phases 1, 2 and 3 as well as the associated documentation. In actuality, the documentation is not a separate phase; instead, it is performed continuously alongside the process of model construction, as described above. The research process is applied to the problem situation to yield the present thesis study.

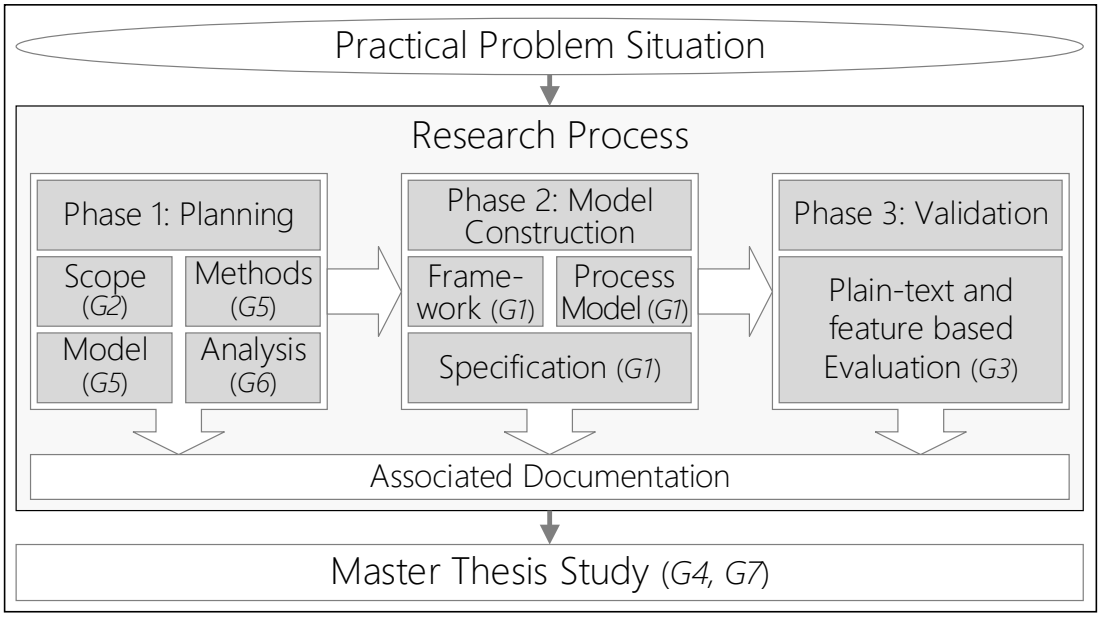


Figure 4: Adapted Model for the Applied Research Methods and Process (own figure)

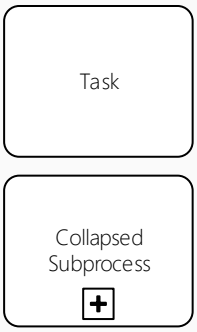
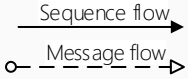
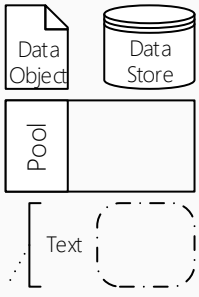
3. 3. 2 Model Annotation and Tool Support

Among the many modelling languages and tools available, business process modelling and notation (BPMN) has been chosen for the construction of the process model. This selection is based on the fact that BPMN in version 2.0 has become the standard notation for business process models (ISO/IEC 19510:2013).

The specification defines several functions and characteristics: namely, what the elements of the models look like, how they are combined, what the model means and how the exchange of diagrams between different tools is done.

The core elements and concepts used during the modelling are introduced in Table 3. The BPMN contains a large number of specified elements, and the intention is to customize the model to cater to the needs of different user groups and situations.

Table 3: BPMN Basic Modelling Symbols

Element	*Notation*	*Description*
Events		This principle models each type of event within a process. The process starts and ends with a respective event element. Many different types of conditions and requirements can be specified additionally. For example, these can be in-/outgoing messages, periodical/timing events, occurring of errors/exceptions and multiple events.
Activities		Activities represent the essential action. A task is an atomic working unit that is performed by one personnel unit. Aggregated activities mark collapsed sub processes and labels with a "+"; meanwhile, expanded sub-processes are composed using a separate and more detailed process.
Gateways		Gateways control the process flow with regards to the specific requirements of the workflow.
Control flow		These elements show the flow through the process and the corresponding messages.
Data Participants Artefacts		Additional elements can be used in order to specify related data objects and stores; they can also assign roles and workgroups. Different perspectives can be addressed as a result of having the opportunity to group some parts of the model together. Additional comments can be helpful.

In general, the core concepts are acceptable for process models from a functional perspective. For the objectives of a reference model to be generally applicable, the modelling notation must be kept as generic and abstract as possible so that there are not too many restrictive details.

The documentation alongside the modelling task in Chapter 5 describes the restrictions and abstractions made. Limitations or room for interpretation are also recorded.

Different software tools are available for supporting the task of modelling and documentation. For the elaboration of the models in this research, Microsoft® Visio® (with the BPMN-shapes) is applied as software support. It should be taken into account that this tool is easily available and widely used and does not demand extensive work from the researcher.

3. 3. 3 Evaluation Criteria for Conceptual Models

The norms selected and the artefacts constructed need to be evaluated in accord with the scientific research process; they also need to meet the research principles shown and specified in the previous sections. Clearly stated criteria are needed for the evaluation of the quality of the artefacts constructed, as the construction of a model contains a singular and individual interpretation of a real-world segment made by the model designer.

The evaluation criteria follow the evaluation method found in "*Descriptive: by Informed Argument*" (Hevner et al., 2004, p. 86). Existing modelling principles have been considered to elaborate the evaluation criteria. These include:

- the generally accepted modelling principles (GOM) (Becker, Rosemann, & Schütte, 1995),
- the improvement of the aforementioned principles (GOM II) (Schütte, 1998, pp. 111–133),
- the ascertainment of the named principles to concrete specialities of reference models as their universality of enterprise-specific information models (Rosemann & Schütte, 1997, p. 31), and
- the critical adaption of the principles to more process-oriented evaluation approaches (Vom Brocke, 2003, p. 148).

The criteria for the subsequent evaluation of the models constructed are defined as follows:

- ***Principle of Adequacy:*** The adequacy assesses how appropriate the content and the representation of the model constructed are in relation to the intended purpose of the model. In this context, both the object developed within the specified context, the content that is described and aspects of the illustration are investigated.

- ***Principle of Profitability:*** The impact on economic goals within an organisation is examined. This helps to assess costs versus benefits associated with the usage of the model.

- ***Principle of Reproducibility:*** The reusability of the models that are elaborated is an important aspect during the development of reference models. This points to the pragmatic facets of the content, the context of the underlying problem, and the used language for the representation.

- ***Principle of Systematic Structure:*** During multi-perspective modelling, consistency must be maintained between different points of view to reduce conflicts between the levels.

Some interdependencies exist between the principles stated above that can result in a conflict of objectives. This point needs to be taken into consideration during the construction process. It can be challenging to create a reasonable balance between the requirements to tackle the problem situation (Schütte, 1998, p. 138).

This chapter described both the research method spectrum applied in the study in a general sense and the reference modelling approach in detail; the chapter also presented how both of these techniques align with the guidelines of design science research. Business process modelling notation was also introduced. Final, the evaluation criteria, which are composed for the analysis of the literature and the evaluation of the models, were stated and explained.

4 Standards and Good Practices

This chapter consists of a comprehensive analysis of existing standards and good practices within the field of IT governance. Some approaches are presented; they are also analysed using the evaluation criteria and summarised, with their individual characteristics highlighted. To derive relevant requirements for model construction, a comparison of the analysed approaches is provided.

4. 1 COBIT 5

4. 1. 1 Characteristics of COBIT 5

A comprehensive and common reference model for IT governance is the COBIT framework. COBIT stands for control objectives for information and related technologies. It was initiated and published in 1996 by the Information Systems Audit and Control Association (ISACA) in cooperation with the IT Governance Institute (ITGI). COBIT is an reference model that is internationally accepted and is currently in version 5 (ISACA, 2012).

With the aid of COBIT, the information goals as defined within the information strategy can be aligned with the general business goals of the company. To measure the output of the related activities, control objectives defines the intended outcome. To realize the intended outcome, controlling procedures must be defined. For this step, COBIT provides comprehensive support to the daily work for managers, users and auditors.

Five basic principles comprise the underlying foundation of the framework. They are, as presented in Figure 5: (1) meeting stakeholder needs, (2) covering the enterprise end-to-end, (3) applying a single integrated framework, (4) facilitating a holistic approach, and (5) separating governance from management. These five principles aim to provide a holistic approach to aligning business with IT as it focuses on an overall view of the company and its key stakeholders concerned. Furthermore, COBIT gives control objectives for each process to support the development of an IT governance framework adapted for all types of companies and organisations. Moreover, COBIT provides activity goals for the purpose of controlling the implemented processes. The end goal is to achieve an improvement in the effectiveness and efficiency of the processes.

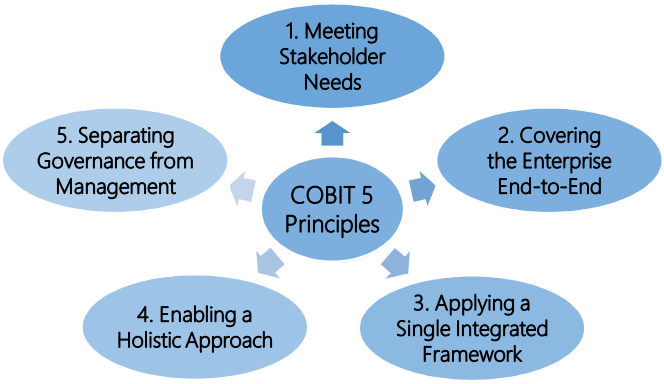


Figure 5: COBIT Principles. Source: ISACA, COBIT 5 2012, p. 13

The goal and performance indicators can be used to measure the outcome of the information processes and to assess them using maturity levels. These can be further used to create a benchmark for comparison with other companies.

4. 1. 2 Analysis of COBIT 5

Principle of Adequacy: The focus on applying a holistic view to the entire business and its related IT is a good basis for the usage in all kinds of companies, including small companies. In addition, the attention given to the stakeholder's needs is critical to the daily business and to information security. COBIT helps the management to develop an adequate structure for the entire company. By employing a language that is currently used for the description of processes, COBIT provides easier access to the message even for inexperienced members in the organisation. Even though the intention of COBIT is to be generic enough for all kinds of enterprises, it has reached to such an extent that it might be too much for a smaller company management to become acquainted with it. This is because its extensive development, the description and the professional guides to the framework. Although the approach provides objectives and documentation for many different processes, it does not show one ideal process for enhancing QISM that is specifically useful to smaller businesses. Nevertheless, it would be helpful to learn more about such management to establish a base for future growth.

In addition, the fifth principle (see Figure 5) may be difficult to follow in smaller companies in which the head of the firm is equally involved in the daily core business, the management of the company, and its management decisions. It is possible for the business owner to focus on the core business personally and to outsource some parts of the IT management. Although the head of the firm is often

only one person, it may be difficult for the head to avoid management decisions on quality management and information security within the company.

Principle of Profitability: The COBIT framework is currently available for purchase and is published in different languages. The professional guides need to be purchased additionally, if necessary. Even though the price for the individual parts of the framework seems to be reasonable, it is costly for small companies. Furthermore, learning the process and working out a process landscape that is individually adapted and customized to the company's needs can generate further expense. According to the educational background of the business owner, this area may require resources that are needed within the core business. Therefore, it is preferable to hire additional staff or to outsource this task. Moreover, to acquire the information essential to the upcoming decisions—what measures are appropriate to the current business—can require a huge effort from the business owner. It appears that the costs can exceed the benefits of implementing such a generic compilation. Nevertheless, if requirements from an external stakeholder necessitate activity, or if the benefit of a reputation established by a well-esteemed certification is highly valued by the enterprise, then action could most likely be taken.

Principle of Reproducibility: The underlying intention of the COBIT framework is to be adaptable to every kind of company. Since the publication provides documentation and objectives for many different business- and IT-related processes, COBIT is widely adaptable even to small companies. The problem situation that is addressed can be detected in almost any kind of business. The modelling language used is plain-text description with a few illustrations. It is easily reproducible. According to this plain-text description, the processes are not automatable directly; they require adaption to the specific needs and tools used by the individual enterprise.

Principle of Systematic Structure: The framework represents a systematic approach used to elaborate an enterprise-individual process landscape. It is also intended to involve both external and internal stakeholders. The templates for process documentation provided facilitate a structured proceeding towards specified maturity levels and objectives. Different points of view are evaluated during the development, and they provide support for handling conflicts. However, it does not provide special visual support to processes. Due to its large extent, the approach can be confusing to smaller businesses, and it may constitute a barrier to enhancement of the QISM instead of supporting the implementation.

4. 1. 3 Interim Summary of COBIT 5 Features

The aforementioned details of the generic COBIT framework for the IT governance within an enterprise are arranged in Table 4.

Table 4: COBIT 5 Summary by Evaluation Criteria

COBIT	*Advantages*	*Disadvantages*
Adequacy	• Holistic approach • Stakeholder involvement • Process-orientation	• Too generic for MSE • Too comprehensive for MSE • Governance and Management
Profitability	• Reasonable pricing • Usable for the whole business and its further growth • Beneficial for reputation	• Matter of expenses • Skill training required • Additional staff or outsourcing • Decisions needs information
Reproducibility	• Adaptable for all kind of enterprises • Example documentation • Plain-text description	• No extensive illustration • No modelling language used • Not directly automatable process model
Structure	• Systematic approach • Cover maturity and control objective measurement • Example documentation	• No process visualisation • High complexity, due to the generic framework • Not easy to get started

Although COBIT 5 provides support for nearly all processes related to the company's business and IT, it may require an overwhelming effort to get the board of an MSE to start on the approach. Although the descriptions in the current version are much easier to understand than in earlier versions, the effort needed to learn how to use the approach appropriately may not be worth the benefits. The publication, *COBIT 5 for Information Security* is meant as a professional guide; it has to be purchased separately and contains a huge amount of information, including relationships between the technical, formal and informal parts of the organisational information system. The information can be overwhelming, and this can pose as a barrier for companies to take the effort to implement this framework to establish a better QISM. This may be especially the case for smaller companies.

4. 2 IT Infrastructure Library (ITIL®)

4. 2. 1 Characteristics of ITIL®

The Office of Government Commerce (OGC) in the United Kingdom has developed ITIL® since the 1980s; at present, there is a requirement for any mention of the term to be expressed as "*ITIL® is a Registered Trade Mark of AXELOS Limited.*"[5] This statement applies for all further uses of ITIL in this paper. The current version is the third version (v. 3). It was published in 2007 and updated with some changes in 2011 into a consistent edition of five books with an official introduction.

ITIL is an approach approved to IT service management. It contains good practices that provide an orientation for companies, and these practices can be adapted to the individual requirements of a specific enterprise. All the approaches, methods and processes described can be used to ensure an optimising alignment of organisational IT in order to support business needs.

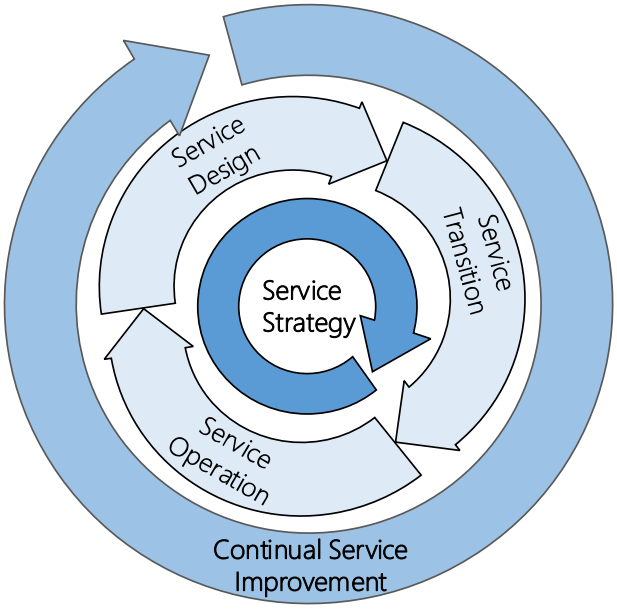


Figure 6: ITIL® Lifecycle, adapted from OGC (2007, p. 19)

Currently, the ITIL views IT service management as a continuous lifecycle. Figure 6 shows this lifecycle. It is composed of service strategy as the core process, while service design, transition and operation build the operational daily business management. All four are embedded in continual service improvement.

[5] See: https://www.axelos.com/policies/legal/copyright-and-trade-marks and http://www.wipo.int/branddb/en/

During the strategic process, which is located in the centre, all strategical decisions are made to align with the operational processes and continual improvement of business goals. The main activities within this part of the circle are financial, demand, and service-portfolio management. The next ring of the lifecycle contains the management processes in relation to the design, implementation and maintenance of the services, which are planned.

In particular, information security management is placed in the service design phase. Continual improvement accompanies all the phases. It is used to heighten the quality of the services provided and to adapt processes to dynamic changes in business requirements.

4. 2. 2 Analysis of ITIL®

Principle of Adequacy: The ITIL provides relevant design principles, purposes and objectives of the activities around IT services at a strategic level. It aims to help management envision all possible consequences and interdependencies. Although it is stated that ITIL could be applicable in all types of enterprises (OGC, 2007, p. 4), the complexity and the level of abstraction with no general solutions seem to be directed towards IT service providers and service delivery centres in larger organisations. The extensive and comprehensive publication with six books may be challenging to smaller companies that intend to implement this approach. Illustrations are used to show relationships at an abstract strategical level and are intended to aid better understanding. For an interested and adequately trained reader, the compilation provides good guidance in the development of an individual IT service portfolio. For a small business with core business outside the IT sector, the ITIL framework may be more than is needed, both in the learning effort and in the adaption process. Even simplifying ITIL and reducing its collection by over 30 specific processes may not be practical for a small company without an IT department. On the other hand, specific parts of the library can provide some orientation that can be used to develop an individual process customized for the company. The ITIL suggests a few key performance indicators (KPI) for every process. These can be used to measure the concrete process progress and outcomes. This trait is particularly appreciated by larger firms, and it makes ITIL the most frequently used framework of those companies who employ an IT Governance framework (ITGI, 2011, pp. 28–29).

Principle of Profitability: The implementation of ITIL can be long term and confusing due to the large dimension of the ITIL framework and its complexity. Consequently, costs are estimated to out-value the benefits. The requirements according to the management of IT services differ in scale and in range between small and large companies. For small companies, it might only be beneficial if customers require such a library. Otherwise, it can be experienced as over-dimensioned. Both the large scope and the great need for consulting due to the unsuitable methodical structure raise fears about a larger effort in internal resources and in training expense for staff. Nevertheless, the approach can provide valuable insights for all kinds of enterprises about how to build a holistic process structure within a company—e.g., how to take the various stakeholders into account and how to measure and develop that structure.

Principle of Reproducibility: The library is not a process model itself; rather, it provides help for creating an individual process structure. This point makes ITIL very useful for many companies and organisations. However, the results of the development of internal processes and structures differ between companies according to their individual requirements. Since the language is plain text and not a specific modelling language, a direct automatization of process structures is not possible. Nevertheless, the library builds a large collection of strategic ideas and guidelines that can be useful in many different settings and complies with this principle.

Principle of Systematic Structure: This is one of the strengths of the latest version of ITIL (version 3 from 2011). The books show a consistent structure so that it is easy to find the right details. The approach as a whole is intended to embrace nearly all possible problem situations within the context of the management of IT services. This holistic view behind the library allows for the integration of specific processes in the big picture of the IT landscape of the firm aligned with business goals. This view also considers different perspectives on IT-related processes; using the key performance indicators, it gives appropriate tools for the monitoring and development of the processes. At the same time, this holistic view at a macro level amounts to enormous complexity. It is not possible to choose only some processes of the library and then to customize those to the needs of a smaller company; this would break down the holistic structure. Rather, a more suitable framework for a smaller scale and different requirements would be better suited to smaller businesses.

4. 2. 3 Interim Summary of ITIL® v.3 2011 Features

Table 5 summarises the aspects of the ITIL framework, as formerly outlined, with focus on the management of IT services including information security management.

Table 5: ITIL v.3 Summary by Evaluation Criteria

ITIL	*Advantages*	*Disadvantages*
Adequacy	• Holistic approach • Stakeholder involvement • Strong process-orientation	• Too generic to MSE • Too comprehensive to MSE • Focus of larger businesses
Profitability	• Usable for the whole business and its further growth • Beneficial for reputation • KPI for the process monitoring	• Matter of long-term expenses • Staff/Skill training required • Additional staff or outsourcing • Unclear pricing and trademark
Reproducibility	• For many enterprises helpful • Plain-text description • Large collection of good practises and strategic guides	• No extensive illustration • No modelling language used • Not directly automatable process models
Structure	• Systematically approach • Cover KPI measurement • Information and dependencies traceable within the books	• No process visualisation • High complexity, due to the generic framework • Not easy to get started

Like COBIT 5, ITIL provides ideas for many processes related to IT services within a company as well as for IT services as a product portfolio, but it seems to be difficult for MSE to get started with it. Even if the use of ITIL is quite common in larger firms, small firms struggle with the complexity and inadequacy of the approach (Wolf & Altgen, 2013, pp. 5–6). However, since ITIL does not provide general solutions for design and implementation of processes for IT service management, it represents neither a standard nor a generally valid ruleset.

4. 3 ISO 9001 and ISO 27001

4. 3. 1 Characteristics of the ISO Standards

The ISO standards have been compiled and are under continuous development by many international members and experienced technical committees. These standards build the internationally accepted basis of certifications and represent the current standard within a specific scope. The ISO 9001 standard in its 2015 version (ISO/IEC 9001:2015) is dedicated to quality management and the related system and requirements. The ISO 27001 in the latest version from 2013 (ISO/IEC 27001:2013) focuses on information security management as a system with technology, technics and requirements.

The ISO 9001 provides strategic help for the improvement of the business and its outcomes related by focusing on products and services offered by the organisation. Its aim is to meet the needs of the key stakeholders concerned and to handle the risks and objectives of the daily business activities (ISO/IEC 9001:2015, p. vi). In order to achieve this, the standard advises adopting a management system that is based on a continuous process approach, which focuses on the establishment, maintenance and improvement of quality within the organisation (ib., p. vii).

Aside from the introduction and application of the aforementioned in section 2. 1. 2, which described the PDSA/PDCA cycle, the ISO 9001 standard (2015, p. viii) shows a schematic single-process example, as presented in Figure 7.

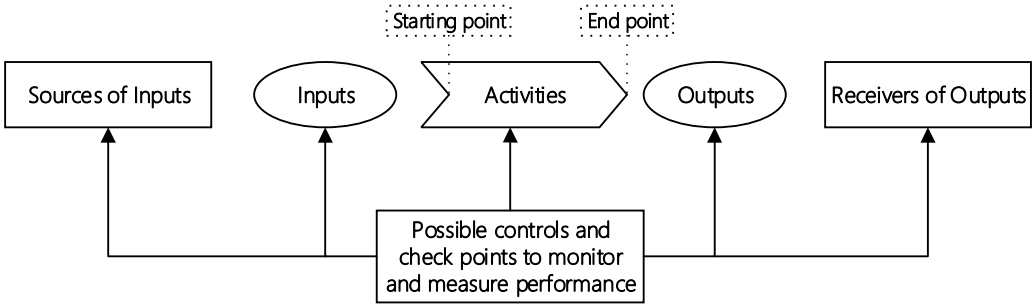


Figure 7: Elements of a single process. Source: ISO 9001:2015, p. viii

Sources of input can be predecessor processes internally as well as externally. Inputs are described as materials, resources and requirements; customer requirements are vital to enhance their satisfaction by meeting their requirements. Outputs of activities include products, services or decisions; the recipients of these are customers, whether internal, external or other (ib.). During the introduction

stage, the ISO 9001 standard gives general notes regarding intended benefits and quality management principles. Moreover, the process approach contains one single process. This includes also its interrelations acting as the continuous lifecycle of the whole quality management system. Comments provides risk-based thinking as an essential enabler of intended achievements. This concept includes taking preventive action to hamper nonconformities, analysing accidents and taking action to prevent the recurrence of such events (ISO/IEC 9001:2015, p. ix).

The ISO 27001 standard describes, "the requirements for establishing, implementing, maintaining and continually improving of an information security management system within the context of the organisation" (ISO/IEC 27001:2013, p. 1). Both standards include requirements regarding the context of the organisation. However, ISO 9001 includes systematic processes that are not specified in the current ISO 27001. Through the requirement specification around organisational leadership, ISO 9001 is much more detailed regarding customer focus by leadership, commitment, roles and responsibilities. In contrast, the ISO 27001 provides specifications on information security risk assessment and treatment. The planning requirements are quite similar in both standards; however, the ISO 9001 contains the planning of changes, unlike ISO 27001. The section about the required support from internal resources to implement the standard is more detailed in the ISO 9001. Requirements targeted to support competence, awareness, communication and documented information are almost identical within both standards. According to the requirements for the operation of the standard, ISO 9001 appears to be more specific in many points regarding (1) operational planning and control; (2) products and services that are internally and externally provided, including their changes and improvements and their provision; and (3), the release and control of nonconforming outputs. The finishing remarks for performance evaluation—such as internal and external audits—and further improvement are almost the same, even if the newer ISO 9001 standard indicates improvement of the specifications. Improvement occurs in general remarks and in the requirement to consider results of evaluations and measures consequently; this is done to improve the needs or opportunities as input in the processes, even in the specification of resources and responsibilities related to the process.

4. 3. 2 Analysis of ISO 9001 / 27001

Principle of Adequacy: The ISO 9001 provides a very generic model of a single process and the process or lifecycle of continuous improvement. The ISO 27001 currently does not show any kind of reference model. Nevertheless, the ISO standards provide many fundamental aspects for the development of different types of business process models. They give valuable perspectives on organisational responsibilities, content related and documentation of relevant processes. Moreover, their requirements may be similar to requirements that stakeholders interested prefer. The standards generate an initial basis for an individual organisation. A holistic view is intended, as the standards are applicable to any kind of organisation. Stakeholder involvement is a central aspect of the ISO 9001. Even though both standards are process-oriented, the ISO 9001 is much more specific about the business resources related to the process (e.g. material, financial and human resources), business process objectives as well as monitoring and development activities. Both standards state what should be considered, but they provide no course for concrete action and offer no process model. Illustrations are almost non-existent, and those that are given are at a general abstraction level.

Principle of Profitability: The ISO standards are easily purchased by standardised pricing. Although the cost of the purchase is not expensive, the implementation may add to the initial costs. Applying the requirements to any particular organisation requires considerable effort to map organisational structure, responsibilities and dependencies. Furthermore, competent staff are in demand as internal resources or as external service providers. Both situations require costs, communication and management effort and entail the risk of information leakage.

On the other hand, this effort and the further implementation of one or both standards can help save costs; such costs can accrue by double work due to a lack of documentation, repeated failure or excess authorisation level. Each organisation can earn benefits by applying both standards to its business in process organisation, effectiveness, information management and customer focus. Since the ISO standards overlap in many places, the cost-effective solution would be to introduce both standards at the same time. If this is not possible, ISO 9001 should be implemented first, as much more effort is needed to implement ISO 27001 if ISO 9001 is not implemented first. This is because ISO 27001 draws on several factors: namely, the facts that the individual process landscape is specified, organisational

responsibilities and authorities are clearly defined, as well as resource usage and information flow is known. ISO 27001 recommends that information security management be anchored within company processes and overall management structures (ISO/IEC 27001:2013, p. v). However, many SME do not deliberately follow any standard. In an uninformed decision to reduce cost, only a quick fix can be chosen. This may not provide a good basis for further development. Such development can be necessary due to further growth of the organisation or exogenous legal requirements. Nevertheless, official certification of the implementation of reputable standards can convey a fair impression to potential future customers or business partners. This might lead to additional growth and enhanced success of the firm.

Principle of Reproducibility: Due to the generic view in the ISO standards, the standards are reusable within all kind of organisations. Since the standards do not provide specific reference models, the business process models developed within various organisations can differ. Yet, the delivery of the requirements might result in similarities within business processes. The ISO standards do not show a path to a good process landscape or information security; rather, they state the objectives that have to be achieved before certification can take place. Therefore, individual business processes need to be specified. The ISO standards are not automatable, as they are written in natural language and neither provide a process model nor are developed with the help of a modelling language.

Principle of Systematic Structure: The focus of the ISO 9001 and 27001 standards is on the alignment between other standards and the requirements of specific aspects, e.g. quality and information security, costumer needs and privacy, of business around the world. The intention is to establish a globally shared terminology and measures regarding QISM systems within organisations. The acceptance of these requirements is assured by the development of the standards by international committees. Otherwise, the standards do not assist in the management of conflicts between interests or different points of view. The only guidance is that such tensions need to be considered and organised in a way that is appropriate to organisational goals.

4. 3. 3 Interim Summary of ISO Standard Features

The ISO 9001 and 27001 standards are equivalent in many statements and have equal characteristics. Therefore, they are considered together in Table 6.

Table 6: ISO 9001 and ISO 27001 Summary by Evaluation Criteria

ISO 9001 ISO 27001	*Advantages*	*Disadvantages*
Adequacy	• Holistic approach • Compatible with other standards and frameworks • Stakeholder involvement • Strong process-orientation	• Too generic for MSE • No aid for concrete action • No help provided for process model development
Profitability	• Usable for the whole business and its further growth • Low initial costs • Beneficial for reputation • Beneficial if established together	• No practical guidance for MSE • Staff/Skill training required • Additional staff or outsourcing • Higher cost if implemented in mistaken chronological order
Reproducibility	• Reusable / Adaptable in all kind of enterprises • Plain-text description • Objectives before certification	• No extensive illustration • No modelling language used • Not directly automatable process models
Structure	• Systematic approach • Alignment to other standards • Globally and commonly used	• No process visualisation • High complexity • Not easy to get started

A benefit of the ISO standards is that their low initial cost allows a business to start with very low risk. Furthermore, the standards do not require the implementation of a specific framework or the approach of a particular supplier. Nor do SME need to hire expensive consulting services either. The requirements as stated by ISO norms do request a level of measures that accords with individual business. It is critical to get started in a structured way and to improve the management system continuously. However, ISO standards do not provide practical guidance for this.

4. 4 IT-Grundschutz by BSI

4. 4. 1 Characteristics of IT-Grundschutz

To increase information security and improve the processes related to it within companies and organisations, BSI has developed a couple of standards that follow the ISO 27001 standard and its requirements. These documents are dedicated to all interested as well as responsible individuals and are available at no charge on the BSI website. The intention is to provide free help and advice for all kind of organisations and to thereby build a better security culture in Germany in general and appropriate ISMS within the business landscape in particular. The distinctive feature—which is found in the BSI-standards and IT-Grundschutz catalogues dedicated to individual aspects of security management—is the aim to give practical guidance in the implementation of the ISO 27001 through specific recommendations. With this characteristic, the BSI Grundschutz is the more practical and procedure-oriented extension of the ISO 27001. Individual technical measures are considered secondary for establishing an appropriate level of information security (BSI, 2008a, p. 5). This means that if the systematic process at the management level is not in place, poor decisions or employees lacking relevant knowledge can lead to weak points in the system so that technical measurements cannot take full effect.

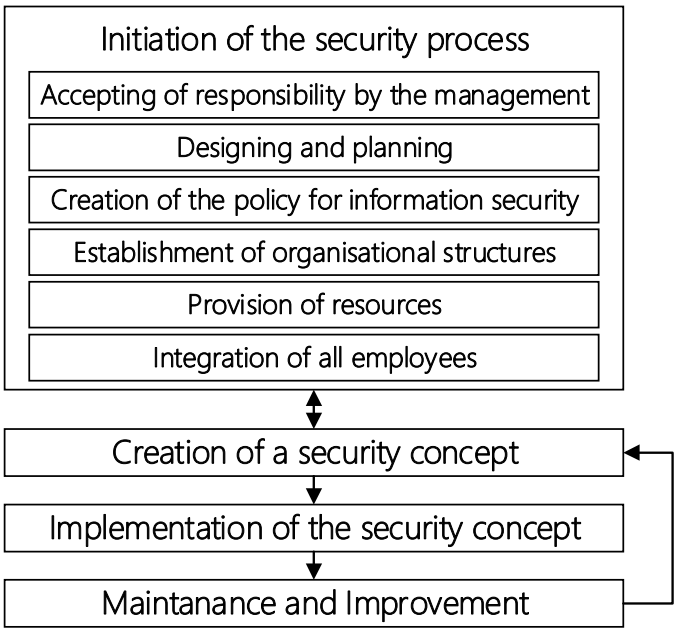


Figure 8: Phases of the BSI Security Process. Source: BSI, 2008b, p. 12.

Figure 8 presents the systematic information security process recommended by BSI. During the BSI Standard 100-2 (2008b), the phases of the process are outlined, and specific actions are described in more detail.

At the starting point, during the first phase of *initiation of the security process*, the management of the organisation has to take responsibility for both, information security and the process. Without this step, the following steps would not provide a good solution in the end; for instance, necessary decisions may not be made in time, or relevant resources may not be dedicated to necessary processes. In the next phase, *creation of a security concept*, a structural analysis of the IT assets, environment and related personnel and information sources is performed. Moreover, protection requirements are determined according to the results of a risk assessment. Other security measures are also part of this phase: namely, decisions around safeguards, security checks, and further security analysis. In the phase, *implementation of the security concept*, the desired level of security is stated and documented; safeguards and monitoring measures are also implemented. By the fourth phase, *maintenance and improvement*, a continuous routine of monitoring and improvement is established to maintain and develop the intended security level and to keep the safeguards adapted to upcoming threats. Lastly, the IT-Grundschutz methodology can be properly used to achieve a certification based on ISO 27001 and based on IT-Grundschutz by an independent external auditor. (BSI, 2008b)

In addition to the BSI standards, catalogues and profiles are available. The 13th version of the IT-Grundschutz Catalogues provides extensive help and guidance to almost all problems, technical situations and safeguards known before printing in 2013. It has been constantly developed and is currently being edited for further improvement according to newer challenges and to reduce complexity. The different profiles provide help adapted to the size of the business. They can provide guidance with respect to the individual realisation, and documentation of the security process tailored to the size of the organisations. These profiles can help facilitate the beginning of the project towards establishing an appropriate level of information security for responsible individuals within the enterprise. This extensive help and guidance is the advantage that could make IT Grundschutz the most commonly used ISMS, followed by the associated ISO 27001 standard (BSI, 2015, p. 29).

4. 4. 2 Analysis of IT-Grundschutz

Principle of Adequacy: The IT-Grundschutz by BSI contains several process models, which, at various abstraction levels, provide an integrated view of the organisation and are dedicated to different purposes and target groups. Despite having the PCDA-lifecycle model accentuating the continuous development of the ISMS and its specific aspects, the IT-Grundschutz provides even simpler process models to highlight the main points during the offered approach. The models are adequate for the purpose of illustrating the security process. Moreover, they are easily comprehensible and do not contain any relations to organisation units, technical systems or other extensive information. This is due to the process-oriented universality of the systematic approach intended to be generally adaptable to any kind of organisation. By the ISO standards generated, IT-Grundschutz extends the general basis to individual organisation by adding guidelines and assistance. This generality is not easily scalable to the situation of smaller companies without a larger management or IT department. Therefore, the profile for small companies gives guidance for the beginning stage and documentation; but aside from illustrations, it does not provide a process model adapted to MSE. Nevertheless, the importance of the IT-Grundschutz lies in its very comprehensive and textual content that is well-structured.

Principle of Profitability: The fact that IT-Grundschutz is available for free on the BSI website gives it a strong advantage. Moreover, the IT-Grundschutz follows the ISO 27001, which is why the ISO 27001 may not need to be purchased either. Nevertheless, as mentioned earlier, the work is not done by getting the information on paper: there needs to be an individual security strategy and documentation up to implementation of security measures, continuous monitoring, and improvement. These activities require internal or external resources that are accompanied by costs. These costs may be high at the beginning and then lower later, but they remain present throughout the process. One cost-effective solution for smaller companies could be that the owner acts as the person responsible, acquires the relevant knowledge, and performs the actions required. However, business owners in smaller companies often have specialist competence in their core business. For this reason, the time needed for owners to invest in learning an area outside of their expertise can cost more than it would to hire an external consultant firm to initialize and manage the ISMS. This requires a relationship of

trust and an appropriate service level agreement. Nevertheless, it is important for business owners of small companies to realize that not all responsibility can be outsourced. As IT-Grundschutz points out in the guideline, the head of the company needs to accept overall responsibility for the organisational information security towards both internal as external stakeholders. As mentioned before, the successful implementation and maintenance of an appropriate level of security helps to save costs in the future. For example, these can be costs due to data loss in consequence of a cyber-Trojan, industrial espionage or data security breach related to the confidential data of a third party. A certification of the ISO 27001 by BSI IT-Grundschutz is possible, and it does create costs through the external audit. On the other hand, this can provide an increase in favourable reputation and trust for the customer in the business practices of the company.

Principle of Reproducibility: Although the models presented are easily reusable due to their generality and plain design, they are not easy to use in reality. The approach expects that management can be done first and can involve all employees; after this, a security concept can be conceived. Until then, the practical aspects are considered and realised. In contrast, real business requires a cost benefit analysis from the beginning, which also requires a structural analysis at the initial stage. In particular, since the service can be outsourced, the process is poorly structured and needs to be adapted to the special needs of organisational decision makers and small companies. The models are not generated by using a specific modelling language; therefore, they are not automatable either.

Principle of Systematic Structure: BSI standards and various guidelines are well-structured, and information can be easily found. However, the models themselves represent more illustration than consequent process models. Parallel execution can occur or the chronological order can differ without having these exceptions modelled; as a result, the consistency is not ideal. The absence of relations to business units means that different points of view are not considered in the models and that multi-perspective modelling—which is used to reduce operational conflicts between views—has not been performed. The textual description of the security process and the measures and procedures are elementary for the understanding of the models. The models are abstract, and they are not appropriate for MSE in a straightforward manner.

4. 4. 3 Interim Summary of IT-Grundschutz

BSI provides free guidance for all kinds of organisations that would like to create a better awareness and an enhanced information-security landscape. Table 7 represents the reviewed characteristics of the BSI IT-Grundschutz and catalogues.

Table 7: IT-Grundschutz Summary by Evaluation Criteria

IT-Grundschutz	*Advantages*	*Disadvantages*
Adequacy	• Holistic approach • Compatible with ISO27001 • Stakeholder involvement • Strong process-orientation • Aid for concrete action	• Too generic for MSE • No adapted process model • Not easily scalable to MSE • Enormous volume of the IT-Grundschutz Catalogues
Profitability	• No initial costs • Scalable to size of company • Beneficial for reputation • Practical guidance for MSE	• Staff/Skill training required • Additional staff or outsourcing
Reproducibility	• Reusable / Adaptable in all kind of enterprises • Plain-text description • Process model appears vague	• No extensive illustration • No modelling language used • Not directly automatable process models
Structure	• Systematic approach • Alignment to ISO 27001 • National common used • Moderate to getting started	• Generic process visualisation • Not adequate model for MSE • No multi-perspective

The intent to provide free information and aid for action to everyone who needs it enables business owners within MSE to get started with information security at a very low cost. This reduces barriers to obtaining proper experience and awareness at a higher level.

Furthermore, a process appropriately adapted and defined to the business can help owners to remain with the project in the midst of their daily business activities. Finally, the risk of misperception of threats to information security is remedied by the actual implementation of the IT-Sicherheitsgesetz in Germany.

4. 5 Analysis: Comparison and Contrast

The models as well as the standards and good practices have been examined. Table 8 concludes the elaboration.

Table 8: Concluded Disadvantages of Standards and Good Practices

	Adequacy	*Profitability*	*Reproducibility*	*Structure*
COBIT 5	• Too generic and comprehensive • Separation of Management and Governance	• Expensive • Skill training needed • Staff or outsourcing	• No adequate process model • No modelling language	• High complexity • High barriers to get started
ITIL v.3	• Too generic and comprehensive • Focus on larger business	• Expensive • Skill training needed • Staff or outsourcing	• No adequate process model • No modelling language	• High complexity • High barriers to get started
ISO 9001 ISO 27001	• Too generic • No aid for activities	• Skill training needed • Staff or outsourcing	• No adequate process model • No modelling language	• High complexity • High barriers to get started
IT-Grund-schutz by BSI	• Too generic and comprehensive • Not easily scalable	• Skill training needed • Staff or outsourcing	• No adequate process model • No modelling language	• High complexity • Moderate barriers to get started

The contribution of the standards and good practices that were investigated to the specific situation within smaller companies has been considered. Now the gap in professional knowledge concerning suitable reference process models for the simultaneous establishment of an appropriate QISM in the context of smaller businesses can be addressed.

The constantly recurring disadvantages within almost all of the investigated standards and approaches can be discerned by the remarks in Table 8. The largest obstacles MSE faces in implementing a common framework can be inferred from the analysis previously performed:

- The **complexity** of the task, due to being too generic and too overwhelming;
- The **high effort** in staff or skill training that is estimated unreasonably; and
- The **absence of** reference **process models,** adequately **adapted,** and guides for the parallel introduction of quality and information security management.

As the results show, the different approaches guide many specific parts of the problem situation. Nevertheless, they are not properly adapted to the preconditions of smaller businesses. It is seen that larger organisations—which consist of many individuals, technical systems and all their relations inside and outside the company—require a clearly structured approach if they are to handle the business and its related communication and coordination. It is not to be taken for granted that MSE may not need a good quality or information security management, as they operate at a much smaller scale.

The largest barrier to using a common best practice or standard is access to knowledge and the ability to adapt at a suitable level to the large amount of information available. However, much effort can be conserved if the quality management *and* the information security management are introduced at the same time. The benefit is considerable in the long run for the firm, particularly if the company grows further; the structures and documentations can help toward continuous improvement and adaption. Furthermore, if process-orientation and customer focus have become a daily habit, the adaption to changes in the business requirements from internal and external stakeholders is much easier to realise in the operational business.

From this analysis and comparison of features as well as and disadvantages of existing standards and good practices in the field, significant requirements are derived. They constitute the basis for the reference model collection to be created, and they are adjusted according to the specific needs of MSE as follows:

- **Holistic view** on the smaller business by a **systematic** approach
- **Stakeholder involvement** by adequate **visualisation** and information
- **Process-orientation** by a reference process model **adapted** to MSE
- **Description** added to process steps with **guidance** for concrete action
- **Alternative solution** for getting started easily at an initial **low cost**

This chapter has analysed and compared relevant standards and good practices in the field. This investigation included COBIT, ITIL, ISO and IT-Grundschutz. Considerable disadvantages could be ascertained. In this way, obstacles were found in the context of smaller organisations. As a result, the requirements for the construction of an appropriate reference model collection are presented, and they constitute the basis for the model construction.

5 Model Collection QISMO

This chapter represents the model collection dedicated to a simultaneous implementation of quality and information security management in small organisations (QISMO). The models are constructed based on the requirements specified in section 4. 5. This model collection consists of three parts. First, the collection presents a framework that provides a basis for communication between key stakeholders concerned about requirements and dependencies. Second, a reference process model aids the implementation process within a small company in collaboration with an external consultancy firm. Finally, a lifecycle model offers assistance in continuous improvement.

5. 1 Integrated Framework of QISMO

5. 1. 1 Representation of the Framework

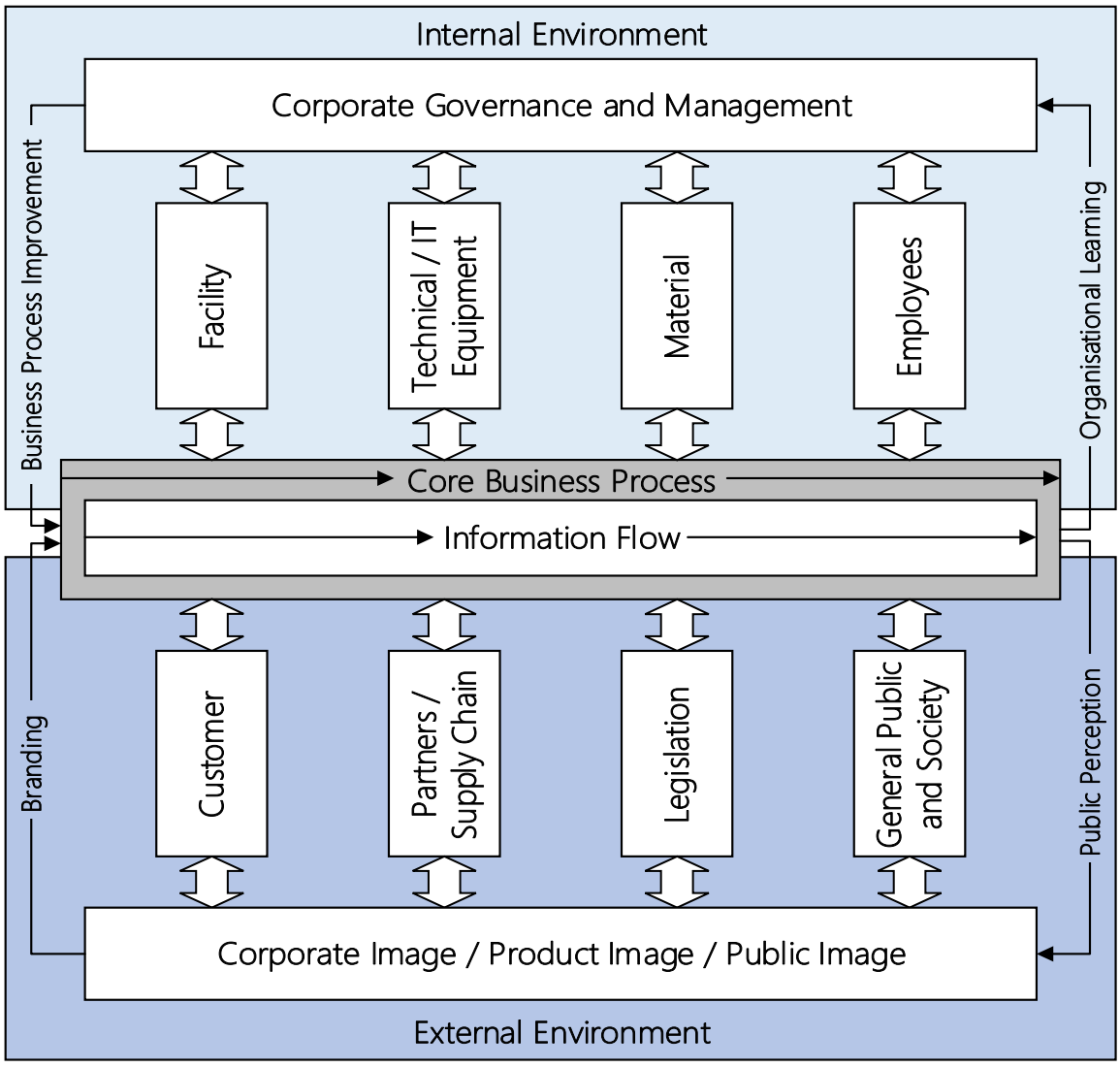


Figure 9: Framework for Quality and Information Security Management for small Organisations (QISMO)

The framework of QISMO constitutes the underlying structure and dependencies of a small organisation, as seen in Figure 9. It integrates internal and external relationships as well as key stakeholders who either influence the business processes of the corporation or are influenced by these processes. The value creation process connects both the internal and the external environment. In an ideal implementation, the information flow runs along defined processes.

The quality management organises the processes, individuals related with them, and material and information flow. In consequence, organisational information security can be managed with less effort when quality management is in place.

5. 1. 2 Specific Parts of the Framework

- ***Internal Environment***

The upper part of the framework illustrates the persons internally involved, resources and the related equipment used to create the product, the service portfolio of the company, or both. The quality of the business processes is determined by the employees, the IT systems and the physical facilities and material input. At the same time, the ongoing process influences these relationships in its turn by unexpected fluctuations and subsequent adaptions. Hence, the new knowledge obtained by such events educates the individuals involved. It also needs to be used for organisational learning and for the deployment of continuous improvement of organisational business processes by the management of both the corporate governance and the information system.

- ***External Environment***

The lower part of the framework comprises the external relationships. The external stakeholders bring expectations and requirements to the company's attention. These stakeholders include; (1) customers; (2) partners and suppliers; (3) legal requirements on products, methods, health and safety of the employees, protection of environment, and data and information; and (4) the wider public. All of these stakeholders are connected with the company and its information system management along the process. These stakeholders influence the process and the resulting product or service. Through public perception, the image of the organisation and its products is created. This point also has a strong influence on the relationships with the external stakeholders. Thus, the customer focus when applied with an appropriate quality and information security management system increases trust in products and services and in the privacy of personal data.

- ***Interface between Internal and External Environment***

Ideally, core business processes constitute the conduit between the internal and the external environment. In the case where the information flow runs well-controlled alongside the designed and documented process, the privacy of information can be monitored and ensured in a proper manner. The requirements of internal and external stakeholders can be aligned and ameliorated continuously according to a corporate governance. This lays the foundation for further adaption. Across the process and information flow, the company can interact with the exterior demands and satisfy challenges. In this way, the organisation influences its public image by developing its corporate brand.

5. 2 Reference Process of QISMO

5. 2. 1 Model of the Reference Process

The reference process of QISMO has been elaborated in strict accord with the design principles outlined in Chapter 3 and with regard to the requirements refined from the analysis as described in section 4. 5. The QISMO framework substantiates the reference process with respect to the underlying structure and dependencies. Moreover, insights obtained from the literature review result in some premises to and restrictions on the designed process.

It is assumed that the business owner within a micro, small or even medium-sized organisation may not be actively engaged in the actual detail-work required to establish QISM within the company. It is also assumed that an external consultant firm conducts the main work, and that the business owner would only participate at a minimal level in these management activities. Because business owners are ultimately responsible for events in and related to their companies, they need to review and authorize the documentation and solutions that has been suggested properly. This involvement of the responsible person within the company has been modelled with the help of message communication.

The reference process is designed at a higher level of abstraction for the benefit of an easier understanding of the process for an audience that may not be experienced in detailed process modelling. Thus, the number of variants of the model elements and sequence flow alternatives have been minimised. To keep the process model clear and easily supervised, the process activities are modelled with a general character and label. Most of them could be decomposed into more detailed sub-processes with more specific actions.

The activities within the reference process model in Figure 10 are displayed in colour to illustrate the process structure and to present the sequence flow in a clear way. The specific parts and elements of the reference model are presented in more detail below.

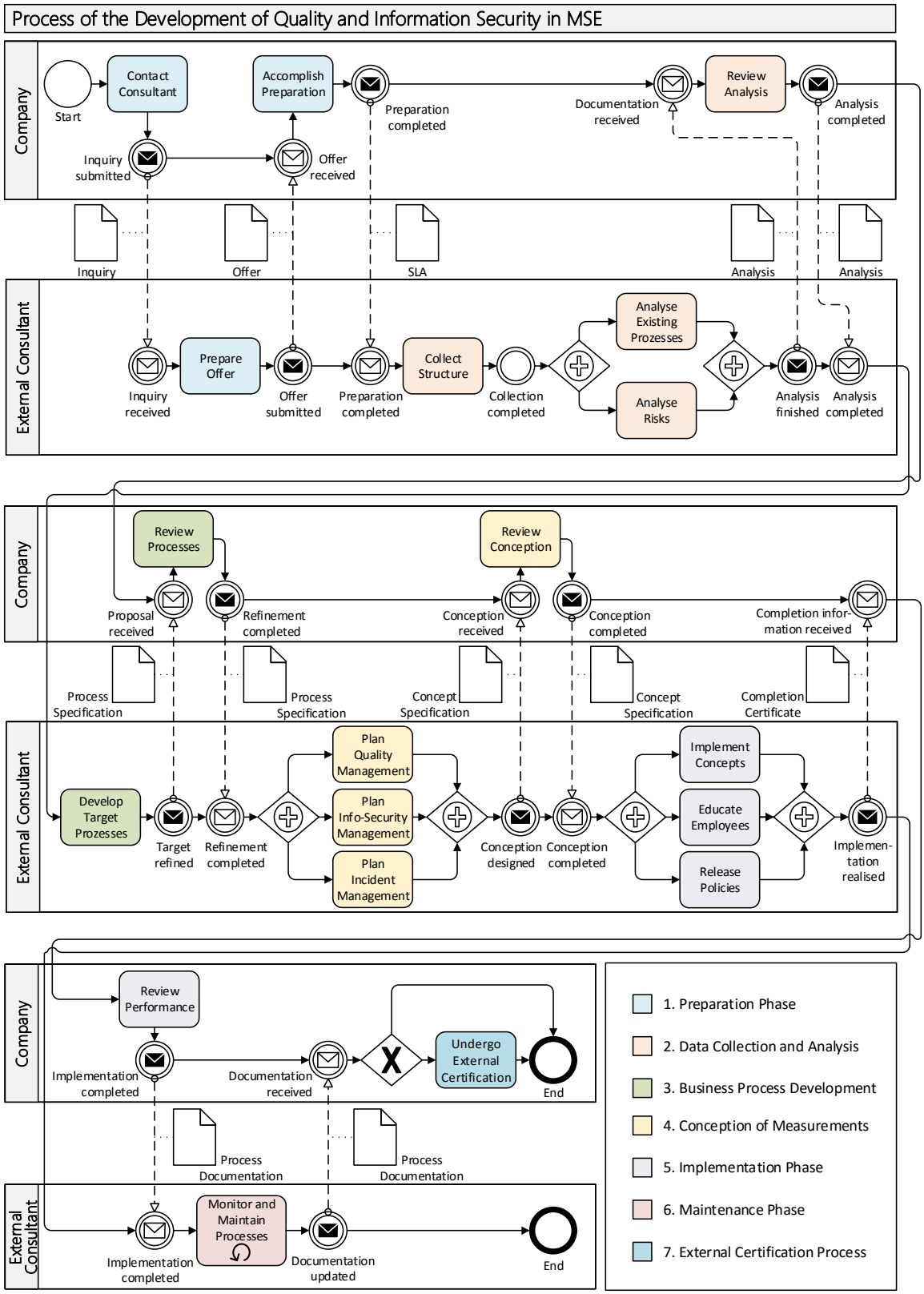


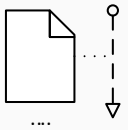
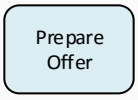
Figure 10: Reference Process for the Simultaneous Development of Quality and Information Security

5. 2. 2 Elements of the Reference Process

The process runs within two lanes showing the individual parts for the two involved partners: one is for the company and is labelled *Company*, while the other is for the external consulting firm (CF) and is labelled *External Consultant*.

Table 9 represents the individual elements of the reference process. Moreover, it remarks specific characteristics related to each element The person responsible for corporate governance in general and for the information system management in particular—usually the owner of the business—is abbreviated as BO in the table.

Table 9: Elements of the Reference Process Model

Nr.	*Elements*	*Description*
1		The process always starts with a *starting event*. This can arise by external requirements—such as initiation by legal regulations or customer requests—or internally by expiration of revision time or the initial start of development.
2		The *control flow* indicates the next element and the possible relations between them within the actual situation.
3		In accord with the premises assumed previously, the first *activity* of the BO is to contact the consulting firm.
4		The itemised *intermediate event*s illustrate the communication between the BO and the consultant by messages. The black message icon represents an outgoing, throwing element that triggers activity for the related partner, who receives the incoming event represented by the white message icon. Intermediate events without specification mark notable events, which are mostly a result of the previous activity.
5		This *data object* represents the documents *associated* to the *data flow*. Informative labelling helps to understand the content and direction of exchange of information and documents.
6		The CF prepares an offer with respect to the incoming order request.

7	Accomplish Preparation	In an ideal process, the review of the offer leads directly to a proper preparation and a service level agreement (SLA).
8	Collect Structure	The next activity for the CF is to collect the physical, technical, formal and informal infrastructure, including investigations previously performed or existing documentation.
9		This gateway displays the possibility of executing the related activities parallel with one another. All activities related to this gateway have to be completed before the repeated use of the gateway merges with the control flow.
10	Analyse Existing Prozesses	As a part of the quality and information security management, the current workflow within the core processes is analysed by the experienced CF to find weaknesses.
11	Analyse Risks	As a part of the information security and quality management, the workflow, infrastructure and related environment need to be investigated for current and potential risks to form a basis for further development.
12	Review Analysis	The BO reviews the analysis report and advises on the specific business and level of security based on the BO's own expertise.
13	Develop Target Prozesses	After the analysis is finished, target processes are developed with respect to the particular and specified requirements.
14	Review Processes	The BO reviews the results accurately. This important task builds the foundation for the subsequent planning steps.
15	Plan Quality Management	The planning of the quality-management concept intended happens in close collaboration with other planning activities.
16	Plan Info-Security Management	The coordination and balancing of the measures for the quality management and information security management are elementary for the practicability and the acceptance within the daily business operations.
17	Plan Incident Management	A plan for problem solving is developed according to the needs of the related business requirements.

18	Review Conception	The BO examines the concept. It is important that the BO understands the details to lead by good example.
19	Implement Concepts	The concepts that was planned are now implemented in its technical, formal and informal aspects.
20	Educate Employees	The education of the employees regarding the changes, new methods and procedures is performed in close connection.
21	Release Policies	Relevant policies for the QISM are released; they are also communicated and explained to employees affected.
22	Review Performance	The performance is evaluated as a completion of the established QISM and the business processes that have been reengineered.
23	Monitor and Maintain Processes	An important activity of continuous QISM is the monitoring and maintenance of the established processes. The updated documentation provides the basis for further certification.
24	X	This decisional gateway represents the exclusive decision between more than one possible way of the control flow. Only one can be chosen.
25	Undergo External Certification	An external or official certification can be passed through if the BO feels that it is needed. The expiry date of a formerly gained certification can be a trigger to start the entire process.
26	End	Regardless of whether the certification is sought or not, the reference process ends here both for the BO and the CF.

The message flow has been kept as concise as possible, and thus the communication elementary for the process success is modelled. Potential communication with a third party is disregarded on purpose for sake of the clarity of the model.

Several activities of the process, which are connected in a logical manner, are grouped in the same colour. This results in seven phases of the process. These can be used to transfer the content of the reference process of QISMO—which contains the underlying structure and dependencies delivered by the framework of QISMO—to a lifecycle to provide a holistic view on the continuity of the assignment within the organisation.

5. 3 Lifecycle of QISMO

5. 3. 1 Model of Continuous Management

Although the reference process model shows the entire process of the development of quality *and* information security within small organisations, the process needs to be anchored in a continuous lifecycle to keep up with ongoing changes of threats and defence strategies. This continual improvement is a part of the management of the company, particularly its information system; it should hence be integrated as a habit in the daily business operations via periodical iteration. Even though it is in the company's own interest to keep the process operating, the external stakeholder—such as legislature and customers—can require continuity, which can be achieved using expiring dates of certifications, for example. Such deadlines are suitable as events for the restart of the process.

As presented in Figure 11, the lifecycle of the process is related to the continuous cycle of quality management as previously presented in section 2. 1. 2. Planning activities constitute a large part in a first run of the process in phases 1 to 4. If the concepts are implemented well in phase 5, potential for improvement can be detected during the monitoring phase in phase 6, which would then form the basis for further action, bringing the process back to the restart point at phase 1.

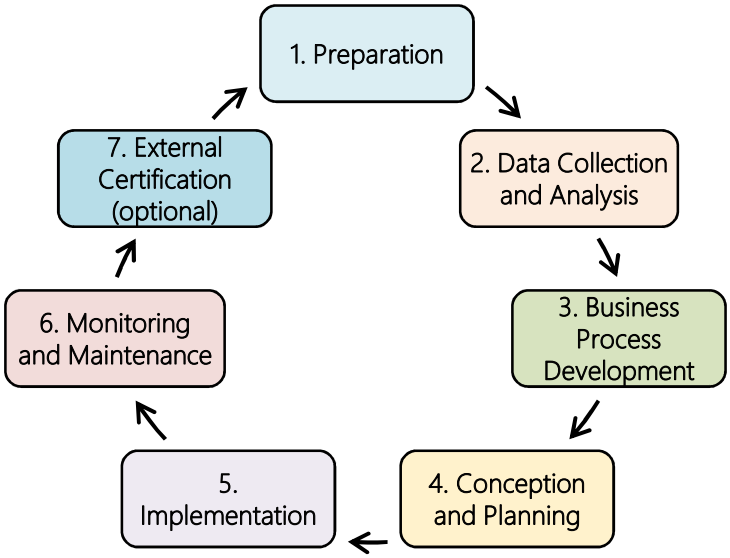


Figure 11: Lifecycle of QISMO

The elements of the lifecycle are presented in detail in the next section.

5. 3. 2 Elements of the Lifecycle

The aforementioned lifecycle dedicated to the continuous management of quality and information security within small organisations comprises seven phases; these are connected in a consecutive cycle.

1. Preparation

During the preparation phase, all activities at the initial stage of the process are performed. Aside from a suitable SLA between business partners related, the preparation of existing documentation and the ascertained problems are also included in this phase.

2. Data Collection and Analysis

This phase contains an inventory of existing structures, resources, related employees, and facilities. After this, the data collected are analysed from a business engineering perspective by an appropriate risk assessment to discover potential weaknesses.

3. Business Process Development

With input from the above analysis, the new processes are created. During this step, it should be considered how risks are manageable alongside the processes and how the business processes are kept as effective and practicable as possible. Otherwise, the employee's acceptance during the implementation phase is elusive.

4. Conception and Planning

The next phase comprises the definition of a proper conception and the planning of upcoming activities. This task includes the balancing and coordination of appropriate quality management actions with the information security measures. Furthermore, responsibilities are specified and a contingency plan needs to be developed for events that are dangerous relative to company requirements.

5. Implementation

At this stage, the processes developed, concepts and measurements that are planned during the previous stage are established in the company's working environment. Especially important, the employees have to be educated properly in a number of areas. These include intended improvements of the business, upcoming changes related to it and the cooperative behaviour expected from the employees during both daily business operations and in case of an unexpected event. To express the liability of this action, adequate policies are released and signed.

6. Monitoring and Maintenance

During this activity, the measurements implemented are continuously monitored, and the level of quality and information security decided within the organisation is maintained. This step runs continuously, or it can also run during a determined time interval as specified in the SLA, for example. Moreover, recurring issues and problem situations discovered are documented in favour of the next iteration of the entire process.

7. External Certification (optional)

The external certification process is actually optional for a majority of smaller organisations. However, further requirements from legal regulatory authorities or even from demanding customers necessitates approved independent certification of processes and measurements related to quality, production processes, and sensitive information.

Continuous QISM does not merely provide a competitive advantage by gaining customer trust and avoiding economic loss. Rather, it enables companies to develop sustainability, both from a business economic perspective for the safety and health of employees, and from a societal perspective for the preservation of the environment.

Chapter 5 has presented and explained the QISMO model collection in an elaborate manner. Structures and dependencies were shown by the framework presented, and the reference model contributes to the proceeding step using a reference process. This operates upon the basis of the framework and connects internal and external stakeholders and various requirements. The lifecycle completes the QISMO family with a condensed perspective on continuous improvement of management activities.

6 Validation of the QISMO Models

This chapter evaluates the QISMO model collection presented. This is performed first by means of the evaluation criteria using the method "descriptive by informed argument", as introduced in section 3. 3. 3. Furthermore, the model collection is then evaluated by several experts with reference to the relevant issues.

6. 1 Evaluation by Criteria

6. 1. 1 Evaluation of QISMO Models by Criteria

Principle of Adequacy: The QISMO framework, the reference process and the lifecycle model constitute valuable resources for organisational development. The methodical approach provides a holistic view of the business, especially within MSE. It enables key stakeholders involved to gain a shared understanding of the relationships and the chronology of the imminent activities. The different points of view and levels of abstraction provide help to various problem issues within communication between target groups involved. This improved communication leads to an enhancement of the management of the processes.

The QISMO models are easily comprehensible and do not require extensive knowledge of process modelling. The models follow a process-oriented approach using the reference process model; they are paired with internal and external structures that are presented by the framework and are completed by a view on continual improvement by the lifecycle. This level of generality is appropriate to the context of MSE and SME. Larger organisations require adaption to their specific requirements, which are often stipulated by regulations, businesses or customers.

This comprehensible model collection illustrates the relations between organisational units, communication and documentation. It also interfaces between responsibilities and individuals in an adequate manner. Relations to technical systems are not included for reasons of clarity and comprehensibility. The QISMO model family extends existing standards and good practices by an approach customised to the special needs of small organisations for QISM.

Principle of Profitability: Since the publishing of this thesis, the QISMO models are available free of charge. This fact constitutes a strong reason to get started with an improvement of management. The concrete reference-process model

enables business owners to calculate in more detail efforts needed in terms of time duration, costs and personnel. This provides help for a better preparation of the upcoming process of the development of an appropriate QISM. Moreover, it assists in further negotiations with external consultants on the service activities specified. As mentioned in section 4. 4. 2, for business owners, it is not necessarily best and most profitable for them to do all work by themselves. Rather, an appropriate outsourcing of relevant activities would be as cost effective as possible. Nevertheless, business owners are ultimately responsible for their businesses and the influence their businesses have on the local environment or society. Therefore, there is a need for cooperation and for a valuable response to the activities. A better active cooperation between stakeholders will amount to a better result of the process and practicable solutions. As a result, high-qualitative attendance leads to a better understanding in a number of areas, particularly in processes that are approved in practice and in a high-quality management, where business owners have gained the ability to act as inspiring examples.

Principle of Reproducibility: The QISMO model collection provides appropriate reusability within the context of micro, small and even medium-sized enterprises. The chronological sequence of activities is adapted to organisations that have not yet established proper management processes. The reference process aligns the activities with an organisational learning process among key stakeholders involved using a clear illustration. Moreover, the process is anchored in the current business by regular feedback. Business owners are responsible for employee participation in the process development. Thus, relevant policies and the education of employees have to be elaborated as a result of the analysis of business processes and risks related to it during the course of business process development and concept planning. QISMO becomes firmly established by the focus on stakeholder education and involvement.

While both the QISMO framework and lifecycle provide illustration and perform a description function without using a specific modelling language, the reference process model is constructed with the help of BPMN. The formal model is easily automated by workflow management systems. It thereby enables the user to apply the decision-making function alongside the explanation and description of the process. Nevertheless, the additional interpretation by an individual observer will reduce potential mistakes.

Principle of Systematic Structure: The well-structured model family punctuates a systematic approach with a multi-perspective view of the problem situation. A detailed description alongside and a clear illustration increases appreciation of the models and the underlying problem situation. The process of the development of an appropriate QISM within small businesses reveals relationships between internal and external stakeholders, which are considered within the models. Points of conflicts are not specially marked, but these can be detected easily by a particular investigation of the models. The QISMO model collection does not provide individual guidance to handle potential conflicts.

6. 1. 2 Summary of Model Evaluation by Criteria

Table 10 displays the summary of the results of the evaluation of QISMO by the evaluation criteria defined in section 3. 3. 3 (*G3*).

Table 10: QISMO Summary by Evaluation Criteria

QISMO	*Advantages*	*Disadvantages*
Adequacy	• Holistic approach • Compatible with standards and good practices • Stakeholder involvement • Strong process-orientation • Aid for concrete action • Adapted to MSE	• Adaption to larger organisation requirements is needed
Profitability	• No initial costs • Scalable to size of company • Enable better cooperation • Practical guidance to MSE	• Staff/Skill training required • Additional staff or outsourcing
Reproducibility	• Reusable / Adaptable • Plain-text description • Framework and lifecycle illustration and description • Formal Process model	• Individual interpretation of an experienced observer recommended
Structure	• Systematic approach • Multi-perspective • Adequate model for MSE • Easy to get started	• Unknown approach • No assistance for conflict handling

6. 2 Evaluation by Experts

6. 2. 1 Conduct of Model Evaluation by Experts

After the plain-text based evaluation using the defined evaluation criteria, experts with relevant knowledge are asked to examine the presented model family. A group of seven experts with different backgrounds have been selected with the intention of gaining a balance in responses.

The group consists of two quality management experts, two information security consultants and three business owners without specific knowledge in neither QISM nor process modelling. In addition, a questionnaire has been sent out to the expert group to obtain relevant insights.

The survey is intended to add rigour (*G5*) to the research and to receive feedback about the following:

Question 1: Does the QISMO model family and the reference process model in particular fit the assigned purpose (Peffers et al., 2006, p. 92)?

Question 2: Is the benefit achieved by the reference model collection recognizable (Fettke & Loos, 2004, p. 1) and appropriate for MSE?

Question 3: Can the application of QISMO offer a larger benefit to the problem situation than secondary approaches (Frank, 2007, p. 119)?

The survey is kept short with minimal formal requirements using the underlying evaluation criteria as *adequacy*, *profitability*, *reproducibility*, and *structure* throughout the individual communication with the experts of the group. This procedure allows for comments and spontaneous suggestions.

In preparation of the survey, the experts were contacted at the beginning of the study. They were asked for permission to hand over the survey at an assigned date. At the time agreed, the questions and the constructed models are sent by email to the experts, whom previously had agreed upon the participation in the evaluation. Furthermore, the email includes the detailed description presented in Chapter 5 and some additional instructions for the further proceeding.

The enquiry suggests the application of a grading scale on each question. The respondents was asked to assess the benefit as perceived individually by using:

(++)	very good,
(+)	good,
(−)	sufficient,
(−−)	insufficient

In addition, some general remarks encourage the experts to express their individual views on the topic using an informal conversation. The responses from the expert group are received through emails, phone calls, and one-to-one conversations. The assessment and comments received from the experts are analysed and compiled anonymously. Since relatively few experts participated in the evaluation, numbers have been allocated to preserve their anonymity. Final, the responses are arranged and the comments considered throughout the next section, and furthermore, in section 7. 2 for the purpose of providing a guideline.

6. 2. 2 Summary of Model Evaluation by Experts

All participants of the survey provided responses owing to the aforementioned preparation. The extent of the comments and suggestions varied, a few are cited below as examples for the feedback received. In general, all experts consider the models to be appropriate to their purposes. Four of the reviewers requested more context about the background of the research paper; in some cases, this was due to foreign language constraints. Furthermore, five experts requested complementary information regarding the secondary approaches. In these cases, insights from the analysis were provided, as discussed in Chapter 4. All of the respondents indicated that they understood the content visualised by the model family.

(6) "*As the models are intended to describe and visualize the processes in a simple manner, they are appropriate to identify and highlight the key aspects to be observed or which require special awareness.*"

A distinct desire was seen for personal discussion and instruction instead of textual communication. The assigned benefit of the models to the business situation differs due to the different backgrounds of the experts. The consultants in quality management found the integrated ISM part to be remarkable, whereas the consultants in ISM were inspired by quality management activities and the aid provided for easier communication with their customers.

(1) "[…] *an organization having any management system already implemented will see the benefit. Others may recognize the advantage of modelling their processes at all and of covering several aspects, like QM, ISM etc. in one turn. It will be even possible to reduce the workload of the management of small companies, since they can focus on items requiring management awareness or decision and delegate standard work instead of personally controlling every single detail of the process.*"

(4) "*I worked for a security company […]. The issue with SME was that they often had reduced IT capabilities, so their security capabilities were often even worse. This made it sometimes hard to explain why specific processes were important, and also to find a good balance between security and actual usability of solutions. This is why reasonable complexity reduction regarding security is very important at this point. Otherwise, the small and medium sized companies would be overwhelmed or would just ignore parts of the proposed processes. Therefore, focusing especially on those companies is quite important and to find something that is tailored to them. This is why your models might be very useful in practice.*"

The business owners met the models with broad acceptance compared with other sophisticated approaches. They anticipated that the models could help to reduce barriers into obstacles and could be a viable option for rethinking management. One individual expected too much effort in relation to the benefit of doing nothing. Barely half of the respondents suggested complementary how-to-use-guidelines.

Table 11 provides an aggregation of the points of view provided by the experts. For the purpose of anonymity, the table refers to the responses as numbers allocated to the respective individual.

Table 11: Summary of the Evaluation by Experts

Respondent / *Question*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
Q 1	++	++	++	++	++	++	++
Q 2	++	+	++	++	−	++	++
Q 3	+	+	++	++	+	++	++

This chapter offered an evaluation of the QISMO model collection. The evaluation was performed first by plain-text based argumentation using the posed criteria and then by experts with reference to the issue. The responses were captured verbally.

7 Discussion

This chapter discusses the content of the paper and its relevance to research and practice. Aside from the discussion of the research approach applied, the results of the study are interrelated with the standards and good practices that was previously analysed. Directions for relevant further research opportunities are addressed at the end of the chapter.

7. 1 Appraisal of the Approach

This study is subject to some procedural limitations. Design science research has been applied as the main approach to the study (Hevner, 2007; Hevner et al., 2004). The research process aligned to this approach follows the process of design-oriented ISR (Österle et al., 2011), as described in Chapter 3.

During the analysis of the literature and related work, the argumentation deploys mainly natural language. Statistical or mathematical methods were not used. The literature selected for analysis was limited due to the wide area of corporate and IT governance. The selection was motivated during the argumentation and anchored in the relevant context. Alteration of the context or the research question could have resulted in another collection of literature; thus, the scope of literature used cannot be considered complete. However, the selection was performed with reasonable diligence to the topic (*G2*). Despite the application of objective criteria, collection of the literature chosen for analysis belies the subjectivity of the author and the research questions.

Since there is a wide range of modelling languages and tools available, a suitable corresponding language was chosen. Although the BPMN is not specifically adapted to this kind of problem situation, it provides modelling elements on an appropriately general basis. The variety of elements used was limited to maintain the generality of the models as a reference model for a larger range of this type of cases. Another choice of a modelling language or tool could have led to another representation. Moreover, changes in the preconditions or limitations formulated can result in different model instances. Likewise, the experience of the model constructor influenced the design of the particular model. (*G1, G6*)

Researchers have extensively discussed the importance of having proper evaluation criteria regarding reference and process models, as was shown in

section 3. 3. 3. The evaluation criteria used to analyse the literature as well as the models constructed in this paper were defined in accordance with the research questions and the method applied for reference process modelling (*G3*). Nevertheless, they are liable to individual interpretation. In order to reduce author bias and to gain a proper research rigour (*G5*), experts were asked to evaluate the models as well (Frank, 2007, p. 138).

The underlying research process requests a diffusion of the artefacts and the research process conducted in order to enable evaluation and improvement of models in science and in practice (Österle et al., 2011, p. 9). This thesis will meet this requirement by scientific publication wherever possible (*G7*).

The research field of modelling in the area of business information systems meets the challenges concerning complex relations between different stakeholder views as well as the discourse on relevant and rigorous research methods. Approaches are needed that, "are suited to address the inherent divergences and the resulting frictions effectively" (Frank et al., 2014, p. 39). Models as an abstraction of a real-world segment open constructive discussion regarding a problem situation between key stakeholders concerned. Thus, a construction of "possible worlds" as an important element in design-oriented research (Frank, 2009, p. 172) provides a basis for communication. Hence, a research project and creativity could be enriched by an expanded spectrum of research methods regarding a specific problem situation (Heusinger, 2013, p. 237f).

Table 12 represents the collocation of the research and the findings of the study.

Table 12: Alignment of the Research with the Findings of the Study

Design-oriented ISR	*Design Science Research*	*Findings of the Study*
Analysis	Guideline 2: Problem Relevance	Foundation of the problem situation (Chapter 2), Analysis of standards (Chapter 4)
Design	Guideline 6: Design as a Search Process	QISMO model collection (Chapter 5)
	Guideline 1: Design as an Artifact	
Evaluation	Guideline 3: Design Evaluation	Evaluation using evaluation criteria and an expert survey (Chapter 6)
	Guideline 5: Research Rigor	
Diffusion	Guideline 4: Research Contributions	Analysis of standards (Chapter 4), QISMO model collection (Chapter 5)
	Communication of Research	Publishing of the thesis study

7. 2 Results of the Study

The investigation of actual literature (*G6*) and the model construction (*G1*) were performed in accord with the method description outlined in Chapter 3. The results are grouped by attributes and discussed critically with reference to the sub-questions, as stated in the beginning of the paper (*G4*).

- Aspect of investigation: Attribute *Major Barriers*

The first barrier regarding the ability of MSE to improve QISM was identified as the consequent miscalculation of risks. The framework presented and models related to it are helpful in understanding the complex process of initiation, maintenance and improvement of a proper level of quality management and information security management simultaneously. As a result, the model family lays the foundation for enhanced decision-making on a structured basis. Moreover, it provides a tool kit that can be used to develop a tenable long-term plan that is suited to the particular requirements of the organisation.

A second barrier for MSE has been discovered as deficiencies in awareness training and education. The results of this study can be used to develop employee training and to create an awareness program that can include the gamification of problem scenarios to improve situational awareness, for example. Furthermore, the model family can be applied to higher education in different subjects and fields. The goal of further usage within this aspect is to raise knowledge regarding the importance and required dimensions of measures related. This can be beneficial to gain a generally increased exposure on the topic as well as this can result in a change of behaviour.

The absence of structured processes and routines was detected as a third barrier to the improvement of MSE's QISM. The deployment of the reference process to a practical problem situation gives concrete help for structuring the business world, particularly in MSE. It can be used to perform the task by business owners or by an external consultant through communication, coordination and contract negotiation. The temporal extent of the single activities is not visible directly, as this relies on the individual requirements of the company and needs to suit the individual cases. The active cooperation of business owners can easily be detected within the reference process model and should lead to participation in communication as well as in process and content development related to QISM.

This is particularly important for them to get essential preconditions for further maintenance and to be able to act as a good example in the day-to-day business operations.

In summary, the QISMO model collection previously presented can be a tool to reduce the lack of organisational measurements in MSE and SME. In this way, it enhances both, the competence and the management of information systems.

- Aspect of investigation: Attribute *Standards and Good Practices*

A comprehensive analysis of the literature selected from common standards and good practices was performed in Chapter 4. It used specified evaluation criteria that led to significant requirements that are particularly relevant to MSE. Nevertheless, it can be worthwhile to consider the criteria separately from the size of the organisation. The presented framework—which provides a basis for understanding interdependencies by systematics—gives a holistic view on dependencies in a small business. Thus, it establishes an alternative to involve key stakeholders concerned. Moreover, the reference process model and the lifecycle model provide applicable visuals and information to clarify the procedure. The process-orientation, which is represented through the reference process model specifically adapted to MSE, can help in communication and comprehension between different stakeholder groups. A description is added for process activities that completes the model family, and elaborate guidelines can be developed to provide aid in choosing individual measurements.

The multi-perspective approach can also be adapted to requirements of larger organisations. Nevertheless, the effort to adjust the QISMO can be too comprehensive with the result that other approaches could fit better. Although the approach presented lowers the barriers to getting started, business owners of MSE have to show adequate commitment to succeed with the tasks.

In short, the QISMO model collection constitutes an alternative solution to common standards and practices. Since it is compatible with other approaches, it can be aligned with external certification requirements. Moreover, it furnishes MSE with low-cost resources to get started with the management work easily.

Table 13 summarizes the results of the performed study regarding specific characteristics of the approaches that was analysed.

Table 13: Comparison of the Approaches

Characteristics of the Approaches	*COBIT*	*ITIL*	*ISO*	*IT-Grundschutz*	*QISMO*
Holistic view	YES	YES	YES	YES	YES
Systematic approach	YES	YES	YES	YES	YES
Stakeholder involvement	YES	YES	YES	YES	YES
Process visualisation	NO	NO	NO	PARTLY	YES
Process-orientation	YES	YES	YES	YES	YES
Modelling language	NO	NO	NO	NO	YES
Reference Process Model	NO	NO	NO	NO	YES
Adapted to MSE	NO	NO	NO	NO	YES
Generally useable	YES	YES	YES	YES	YES
Beneficial for reputation	YES	YES	YES	YES	NOT YET
Extent	LARGE	LARGE	SMALL	LARGE	MEDIUM
Complexity	HIGH	HIGH	HIGH	HIGH	MEDIUM
Instruction/ Guide	YES	YES	NO	YES	YES
Costs	HIGH	HIGH	MEDIUM	LOW	LOW
Starting conditions	HIGH	HIGH	HIGH	MEDIUM	LOW

- Aspect of investigation: Attribute *Qismo Model Collection*

The integrated framework provides the structure of interests related to the information from the firm and its business processes. These aspects are vital for managing the organisational information system and the corporate governance. By using the framework, interdependencies and influences on and by information can be considered; as a result, a shared understanding between stakeholders can be achieved. These interdependent influences can be identified and measures can be taken to improve business processes and the brand of the organisation, as external perceived, according to the corporate governance. The framework is constructed as a holistic view on the strategic situation within MSE. A modelling language has not been used to create this visualisation. Moreover, the focus lies

on the alignment of information about business processes. Another choice of focus can result in another representation.

The reference process shows the entire process for simultaneously initiating proper quality management and information security management in small organisations. Although limitations and preconditions have been clearly stated alongside the model origination, modifications of the variables can lead to modifications within the process. Furthermore, the process model has been constructed as a reference model that is general to this type of cases. This implies that certain adaptions to an individual problem situation may be needed to shape an individual instance of the reference process model. In this context, additional activities can be required or the sequential order would be altered. In contrast to other approaches, the paper presents a unique reference model that has been constructed using the modelling language BPMN. While this formal process model is automatable, individual interpretation by an observer having relevant experience is recommended.

The lifecycle of QISMO brings the significant phases of the reference process for MSE together and highlights the continuity in the management of the information system by the circular pattern. The description of the separate parts of the lifecycle completes the model. Additional guidelines can aid specific situations.

Since QISMO model collection is compatible with other common standards and good practices, it could be combined with technical guidelines that are appropriate to individual situations (e.g., for security measurements: Schilling & Werners, 2016, p. 324; Clarke, 2015, p. 541.) Even though the context is initially given for MSE, QISMO can also be adapted to conditions of larger organisations. Furthermore, the premise of legal requirements in Germany can be adjusted to other countries. It is easily applicable to other legal and environmental conditions.

- Aspect of investigation: Attribute *Implications for Practice*

The QISMO model family provides a basis for strategical and tactical planning, and a means throughout implementation and maintenance of the management process. The investigation of the major barriers has demonstrated that the lack of competence and structured processes within MSE can be mitigated by development of approaches adapted to MSE and further guidelines. Furthermore, the evaluation by experts, discussed in Chapter 6, indicated that proper communication—about the steps how the model collection can be used systematically—can be beneficial. Following, a how-to-use guide serves as suggestion for action to business owners.

Step One: Strategical Planning

(1) The integrated framework can be used as a map to find out and reflect about stakeholders, information flow, and their interdependencies in relation to the individual situation in the company. Furthermore, it provides a tool to become clearly aware of the goals of the organisation, both long-term and short-term.

(2) The reference process is generally usable for the implementation of a QISM. This process may needs to be adapted to requirements of a current company, depending on which aspects the business owner outsources to a consultant firm.

(3) The lifecycle model enables the MSE to establish a quick overview on the process and its main activities. Moreover, it can help to renew the competence of the person responsible before each new iteration of the process loop.

Step Two: Tactical Planning

(1) The integrated framework supports the focus on currently relevant objectives. Moreover, the model can be used to plan the appropriate allocation of resources.

(2) The reference process enables to plan the provision of resources and the most suitable time for implementation. Moreover, it can be used as guide for negotiating with consulting firms about the content of services requested, such as necessary documentation, technical measures, routines and policies.

(3) The lifecycle model can be used as quick guide to keep the project on track.

Step Three: During the Process

(1) The integrated framework enhances the communication with the consultant about the objectives pursued of the business and enables a shared understanding.

(2) The reference process enables the regular progress check of the performed and the remaining activities. By this, it can be used to update the tactical planning.

(3) The lifecycle model provides milestones usable for interim billing of services purchased. Furthermore, it helps to revise the process after implementation. Difficulties observed and necessary modifications should be documented. These insights gained from this step provide the basis for the next iteration.

7. 3 Directions for Further Research

Additional issues for further research can be deducted from this study. The research methodology regarding information systems and system modelling as well as system development is subject to ongoing discussion and observance within both traditional and newer research papers. One particularly interesting point is that the design of artefacts as cognitive constructs of a possible future scenario

is a departure from traditional evaluation and testing methods. In this context, further elaborations are suggested on adequate and approved methodology anchored in appropriate research rigour.

In a similar vein, an interesting assignment would be to conflate behaviouristics with design-oriented research even beyond the boundaries of specialist areas. Consequently, knowledge on existing solutions can provide insights that can be used to deduce a concrete need for action and at the same time promote evaluation and improvement of artefacts innovatively constructed (Österle et al., 2011).

Moreover, the originated models can be subject to a larger empirical validation. Interview studies can be conducted before, alongside or after implementation among employees. Field studies can be performed among process instances implemented within MSE. Even an adaption to a larger organisation could form a suggestion for further investigation. In addition to this, another research method, such as action design research (Sein, Henfridsson, Purao, Rossi, & Lindgren, 2011), can be applied to achieve further improvement of the QISMO model collection by iteration and active cooperation with key stakeholders related.

The elaboration of key performance indicators for process measurements adapted to an individual business situation and guidelines for conflict handling between parties concerned could expand QISMO model collection further. Detailed sub-processes can be designed to clarify the reference process steps using the included activities. Checklists adapted to MSE can help business owners control the progress.

The survey alongside the evaluation and literature analysis provides valuable insight into real problems, such as a recurring demand for better education and instruction. Thus, the development of a reasonably consistent education and adequate training dedicated to employees affected, business owners, and students in higher education programs seems to be another relevant topic.

This Chapter positioned the current research within the relevant state-of-the-art research literature in the field. In the first part, the approach applied was discussed in detail. The second paragraph criticised the results of the study in light of the aspects of investigation. The discussion reviewed the major barriers, the comparison of standards and good practices, the QISMO model collection and its usability. Reflections on further research completes this chapter. The next chapter concludes the work and connects the research questions with their answers in the paper. The summary showed the contributions of the work for research and practice.

8 Conclusion

This thesis presents the origination of a model collection, called QISMO, dedicated to the task of a simultaneous initiation of quality *and* information security management in the context of MSE. The QISMO model collection consists of three parts. First, a framework illustrates the information flow related to business processes and key stakeholders concerned. Second, a reference process model visualises the sequence flow of the main activities that are necessary for the task. Lastly, a lifecycle model expresses the continuity of the whole approach. The detailed description of the activities and the phases provides guidance throughout the approach to key stakeholders concerned and readers interested in the topic.

After an introduction to the problem situation, the study outlines relevant background of IT governance with a specific perspective on issues regarding information security in MSE and model building theory. From this, standards and best practises were selected and then analysed by applying defined evaluation criteria. The results are elaborated requirements to the model construction. These requirements were merged with the specifications of the initial problem situation, and the models were constructed with respect to these preconditions. Additional documentation clarified the relevant details alongside the modelling method applied and the model presentation. The models were evaluated using the mentioned evaluation criteria and a questionnaire answered by experts. Subsequently, the discussion of relevant aspects of the study discovered opportunities and limitations related to the chosen context and other approaches. This discussion reviews the QISMO model collection and even the underlying research method in contrast to the literature. Moreover, aspects for further research became apparent.

In the course of the study, the research also focused on answering the research questions posed in section 3. 3. 3.

- *How can an integrated framework and a reference process model be created to simultaneously initiate quality management and information security management in MSE?*

Chapter 5 addressed this question in detail. Furthermore, the evaluation in Chapter 6 and the discussion in Chapter 7 provide details and insights in relation to contexts, opportunities and limitations of the reference model family.

- *What are the major barriers for MSE in the case of the preparation and implementation of an appropriate level of information security?*

The major barriers found are miscalculation of risks; deficiencies in awareness, training and education; and the absence of structured processes and routines. These barriers are characterised in section 2. 2. 3.

- *How can these obstacles be affected to overcome them?*

This question is subject to investigation in several sections within the study. The aid that the QISMO model collection can provide to this problem is reflected on in section 7. 2.

- *Which standards and good practices exist, and what distinctions and possible deficiencies can be identified?*

A collection of standards and good practices related to the given problem situation was selected in section 2. 1. 1. Chapter 4 acquires comprehensive knowledge by means of description and analysis of those approaches.

- *Which elements contain an appropriate reference process model?*

Activities and events related to the task of simultaneous initiation of QISM within small organisations are shown in section 5. 2. Moreover, a description of all elements facilitates the understanding of the reader.

- *What recommendations for action can be derived from the survey?*

The answer to this question is considered during the analysis of the problem situation and the literature as well as the discussion in Chapter 7 in general. Section 7. 2 presents a how-to-use guide as a suggestion in particular.

In summary, this thesis emphasizes a unique perspective on restricted aspects of a wide research field. A different lens could result in another view and can be part of further research. The contributions of this work are the insights that can be added to the current knowledge in order to reduce the gap. On the one hand, the valuable discoveries on human behaviour and relating barriers to enhancing information security can be used to develop adequate education and training. On the other hand, the knowledge derived from the elaborated analysis of existing literature, standards and good practices provides guidance and background to an audience interested in the field. Lastly, the reference process model can be reused in other problem situations in practice or research as well as during education.

Publication Bibliography

ATKearney (2012). *Großunternehmen ignorieren die Gefahren durch Hacker und Wirtschaftsspione.* Düsseldorf. Retrieved February 28, 2016, from ATKearney: https://www.atkearney.de/documents/856314/1214356/PM_informationssicherheit.pdf/6cc21f17-6e01-40c5-af9c-fd334b3631d8.

Ahlemann, F., & Gastl, H. (2007). Process Model for an Empiracally Grounded Reference Model Construction. In P. Fettke & P. Loos (Eds.), *Reference modeling for business systems analysis* (pp. 77–97). Hershey, PA: Idea Group Pub.

Aziri, B. (2015). Managing Quality: With Special Emphasis on SME's in the Pollog Region. *Journal of International Scientific Publications, 9*, 337–342.

Barlette, Y., & Fomin, V. V. (2008). Exploring the Suitability of IS Security Management Standards for SMEs. In R. H. Sprague (Ed.), *Proceedings of the 41st Annual Hawaii International Conference on System Sciences. Waikoloa, Big Island, Hawaii* (p. 308). Los Alamitos, Calif.: IEEE Computer Society Press.

Bayerisches Staatsministerium für Wirtschaft und Medien, Energie und Technologie (Ed.) (2012). *Qualitätsmanagement für kleine und mittlere Unternehmen.* München.

Becker, J., Rosemann, M., & Schütte, R. (1995). Grundsätze ordnungsmäßiger Modellierung. *WIRTSCHAFTSINFORMATIK, 37*(5), 435–445.

Bertalanffy, L. von (1968). *General System Theory: Foundations, Development, Applications.* New York, NY: George Braziller.

Boulding, K. E. (1956). General systems theory - The skeleton of science. *Management Science, 2*(3), 197–208.

Bourne, V. (2014). *Risk:Value Report: Do senior executives understand their role in data security?* NTT Com Security. Retrieved May 28, 2016, from http://www.nttcomsecurity.com/en/uploads/files/UK_White%20Paper_Risk%20Value_Public%20Approved_%20V3.pdf.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2008a). *BSI-Standard 100-1 - Information Security Management Systems (ISMS).* Bonn. Retrieved February 27, 2016, from https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzInternational/itgrundschutzinternational_node.html.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2008b). *BSI-Standard 100-2 - IT-Grundschutz Methodology.* Bonn. Retrieved February 27, 2016, from https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzInternational/itgrundschutzinternational_node.html.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2009). *Informationssicherheit: Ein Vergleich von Standards und Rahmenwerken.* Bonn. Retrieved February 28, 2016, from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/studie_ueberblick-standards.pdf.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2011). *Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen (KMU): Grad der Sensibilisierung des Mittelstandes in Deutschland.* Bonn. Retrieved January 16, 2016, from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2014). *Ergebnisse der Cyber-Sicherheits-Umfrage 2014.* Bonn. Retrieved December 07, 2015, from https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/cybersicherheitslage/umfrage2014_ergebnisse.pdf.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2015). *Cyber-Sicherheits-Umfrage 2015 - Ergebnisse.* Retrieved January 16, 2016, from https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/cybersicherheitslage/umfrage2015_ergebnisse.pdf.

Bundesministerium für Wirtschaft und Technologie (BMWi) (2012). *IT-Sicherheitsniveau in kleinen und mittleren Unternehmen.* Retrieved January 20, 2016, from http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/studie-it-sicherheit,property%3Dpdf,bereich%3Dbmwi2012,sprache%3Dde,rwb%3Dtrue.pdf.

Clarke, R. (2015). The prospects of easier security for small organisations and consumers. *Computer Law & Security Review, 31*(4), 538–552.

Deming, W. E. (1986). *Out of the crisis* (26. print). Cambridge, Mass.: Massachusetts Institute of Technology, Center for Advanced Engineering Study.

Deming, W. E. (1993). *The new economics for industry, government, education.* Cambridge, MA: The MIT Press.

DESTATIS (2015a). *Gesamtwirtschaft & Umwelt - Unternehmensregister.* Retrieved December 06, 2015, from Statistisches Bundesamt: https://www.destatis.de/DE/ZahlenFakten/GesamtwirtschaftUmwelt/UnternehmenHandwerk/Unternehmensregister/Tabellen/UnternehmenBeschaeftigtengroessenklassenWZ08.html.

DESTATIS (2015b). *Gesamtwirtschaft & Umwelt - Unternehmensregister.* Retrieved December 05, 2015, from Statistisches Bundesamt: https://www.destatis.de/DE/ZahlenFakten/GesamtwirtschaftUmwelt/UnternehmenHandwerk/Unternehmensregister/Tabellen/UnternehmenUmsatzgroessenklassenWZ08.html.

Dong, P., Han, Y., Guo, X., & Xie, F. (2015). A Systematic Review of Studies on Cyber Physical System Security. *International Journal of Security and Its Applications, 9*(1), 155–164.

Emery, F. E., & Trist, E. L. (1960). Socio-technical systems. In C. W. Churchman & M. Verhulst (Eds.), *Management Science Models and Techniques* (2nd ed., pp. 83–97). Pergamon.

Eurostat (2015). *Business economy - size class analysis - Statistics Explained.* Retrieved December 06, 2015, from Statistical office of the European Union: http://ec.europa.eu/eurostat/statistics-explained/index.php/Business_economy_-_size_class_analysis.

Fettke, P., & Loos, P. (2003). Multiperspective Evaluation of Reference Models – Towards a Framework. In M. A. Jeusfeld & Ó. (. Pastor (Eds.), *LNCS 2814 - Conceptual Modeling for Novel Application Domains* (Vol. 2814, pp. 80–91). Berlin, Heidelberg: Springer.

Fettke, P., & Loos, P. (2004). *Entwicklung eines Bezugsrahmens zur Evaluierung von Referenzmodellen -- Langfassung eines Beitrages* (Working Papers of the Research Group Information Systems & Management No. 20). Mainz. Retrieved March 05, 2016, from http://www.uni-saarland.de/fileadmin/user_upload/Professoren/fr13_ProfLoos/isym_paper_020.pdf.

Fischer, T., Biskup, H., & Müller-Luschnat, G. (1998). Begriffliche Grundlagen für Vorgehensmodelle. In R. Kneuper, G. Müller-Luschnat, & A. Oberweis (Eds.), *Vorgehensmodelle für die betriebliche Anwendungsentwicklung* (pp. 13–31). Wiesbaden: Vieweg+Teubner Verlag.

Fox, D. (2003). Security Awareness. *Datenschutz und Datensicherheit, 27*(11), 676–680.

Frank, U. (2006). *Towards a Pluralistic Conception of Research Methods in Information Systems Research* (ICB Report No. No.7). Universität Duisburg Essen. Retrieved November 15, 2015, from http://www.icb.uni-due.de/fileadmin/ICB/research/research_reports/ICBReport07.pdf.

Frank, U. (2009). Die Konstruktion möglicher Welten als Chance und Herausforderung der Wirtschaftsinformatik. In J. Becker, H. Krcmar, & B. Niehaves (Eds.), *Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik* (pp. 161–173). Heidelberg: Physica-Verlag HD.

Frank, U. (2007). Evaluation of Reference Models. In P. Fettke & P. Loos (Eds.), *Reference modeling for business systems analysis* (pp. 118–140). Hershey, PA: Idea Group Pub.

Frank, U., Strecker, S., Fettke, P., Vom Brocke, J., Becker, J., & Sinz, E. (2014). The Research Field "Modeling Business Information Systems". *Business & Information Systems Engineering, 6*(1), 39–43. Retrieved April 30, 2016.

Grant, K., Edgar, D., Sukumar, A., & Meyer, M. (2014). 'Risky business': Perceptions of e-business risk by UK small and medium sized enterprises (SMEs). *International Journal of Information Management, 34*(2), 99–122.

Grochla, E. (1974). Systemtheoretisch-kybernetische Modellbildung betrieblicher Systeme. In E. Grochla, H. Fuchs, & H. Lehmann (Eds.), *Schmalenbachs Zeitschrift für*

betriebswirtschaftliche Forschung. Sonderh: Vol. 3. Systemtheorie und Betrieb (pp. 11–22). Opladen: Westdt. Verlag.

Gutenberg, E. (1983). *Grundlagen der Betriebswirtschaftslehre* (24., unveränd. Aufl.). Berlin: Springer.

Heier, D. A., & Garret, G. W. (2015). Evaluating Results of a Small Business Security Survey. In V. Bhargava (Ed.),. *Proceedings of the Society of Business, Industry and Economics (SOBIE) Annual Meetings April 14 – 17, 2015 Destin, Florida* (pp. 34–44).

Heitmann, M. (2007). *IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie* (1. Aufl.). *DuD-Fachbeiträge.* Wiesbaden: Springer.

Henderson, J. C., & Venkatraman, H. (1999). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal, 38*(2.3), 472–484.

Heusinger, J. M. (2013). Challenges of Critical and Emancipatory Design Science Research:: The Design of 'Possible Worlds' as Response. In S. Hammoudi, J. Cordeiro, L. A. Maciaszek, & J. Filipe (Eds.), *Proceedings of the 15th International Conference on Enterprise Information Systems, ICEIS 2013, July 4-7 2013* (pp. 233–239). Angers.

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems, 19*(2).

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1), 75–105.

ISACA (2012). *COBIT 5: A business framework for the governance and management of enterprise IT.* Rolling Meadows, IL USA: ISACA.

ISO/IEC 19510:2013 (2013). *Information technology -- Object Management Group Business Process Model and Notation.* Geneva, Switzerland. Retrieved December 26, 2015, from ISO/IEC: http://www.iso.org.

ISO/IEC 27001:2013 (2013). *Information technology -- Security techniques -- Information security management system -- Requirements.* Geneva, Switzerland. Retrieved February 19, 2016, from ISO/IEC: http://www.iso.org.

ISO/IEC 9001:2015 (2015). *Quality management systems -- Requirements.* Geneva, Switzerland. Retrieved February 19, 2016, from ISO/IEC: http://www.iso.org.

ITGI (2006). *Information security governance: Guidance for boards of directors and executive management* (2nd ed.). Rolling Meadows, Ill.: IT Governance Institute.

ITGI (2011). *Global Status Report on the Governance of Enterprise IT (Geit)—2011.* Rolling Meadows, IL USA. Retrieved February 13, 2016, from http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-2011_res_Eng_0111.pdf.

Johannsen, W., & Goeken, M. (2007). *Referenzmodelle für IT-Governance: Strategische Effektivität und Effizienz mit COBIT, ITIL & Co.* (1. Auflage). Heidelberg: dpunkt.verlag.

Jonsson, P., & Wehrmann, A. (2015). *Informationssäkerhet i små och medelstora företag: Examensarbete i Informatik.* Kandidat inriktning Informationslogistik, Linnéuniversity, Kalmar Växjö. Retrieved January 16, 2016, from http://lnu.diva-portal.org/smash/get/diva2:819399/FULLTEXT01.pdf.

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security, 61*, 46–58.

Kim, S. H., Wang, Q.-H., & Ullrich, J. B. (2012). A comparative study of cyberattacks. *Communications of the ACM, 55*(3), 66–73.

Kosiol, E. (1964). Betriebswirtschaftslehre und Unternehmensforschung : Eine Untersuchung ihrerStandorte und Beziehungen auf wissenschaftstheoretischer Grundlage. *Zeitschrift für Betriebswirtschaft, 34*(12), 743–762.

Liebmann, H. P., & Kraigher-Krainer, J. (2003). *Der Zusammenhang zwischen Kognitionen, Emotionen und Stimmungen im Wissensmanagement. Bestandsaufnahme und Entwicklung eines theoretischen Bezugsrahmens* (working papers of the Institute of Marketing). University Graz. Retrieved December 06, 2015, from http://osiv.telesis.eu/download/54_zh_zw_emotionen_und_stimmungen.pdf.

Mendling, J., Reijers, H. A., & van der Aalst, W.M.P. (2010). Seven process modeling guidelines (7PMG). *Information and Software Technology, 52*(2), 127–136.

Mishra, S., Caputo, D. J., Leone, G. J., Kohun, F. G., & Draus, P. J. (2014). The Role Of Awareness And Communications In Information Security Management: A Health Care Information Systems Perspective. *International Journal of Management & Information Systems (IJMIS), 18*(2), 139–148.

Mumford, E. (2006). The story of socio-technical design: reflections on its successes, failures and potential. *Information Systems Journal*. (16), 317–342.

Nofer, M., Hinz, O., Muntermann, J., & Roßnagel, H. (2014). The Economic Impact of Privacy Violations and Security Breaches. *Business & Information Systems Engineering, 6*(6), 339–348.

Office of Government Commerce (2007). *The official introduction to the ITIL service lifecycle.* London: Stationery Office/TSO.

Organisation for Economic Co-Operation and Development (OECD / OCDE) (Ed.) (2004). *Principles of Corporate Governance.* Retrieved January 31, 2016, from http://www.oecd.org/corporate/ca/corporategovernanceprinciples/31557724.pdf.

Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., et al. (2011). Memorandum on design-oriented information systems research. *European Journal of Information Systems*. (20), 7–10.

Palvia, P., Mao, E., Salam, A. F., & Soliman, K. S. (2003). Management Information Systems Research: What's There in a Methodology? *Communications of the ACM*. (11), 289–309.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). The Design Science Research Process: a Modell for Producing and Presenting Information Systems research. In *DESRIST 2006, CGU,* pp. 83–106. Claremont, CA.

Pfeiffer, D., & Niehaves, B. (2005). Evaluation of conceptual models -- a structuralist approach. In D. Bartmann, F. Rajola, J. Kallinikos, D. E. Avison, R. Winter, P. Ein-Dor, et al. (Eds.), *Proceedings of the 13th European Conference on Information Systems, ECIS 2005, Regensburg, Germany,* pp. 459–470.

Reeg, T. (2011). *Modellierung betrieblicher Informationssicherheit: Entwicklung einer geschäftsprozessgetriebenen Modellierungsmethodik unter Nutzung eines Referenzmodells.* Dissertation, Otto-Friedrich-Universität, Bamberg.

Reiter, C. (1999). Toolbasierte Referenzmodellierung — State-of-the-Art und Entwicklungstrends. In J. Becker, M. Rosemann, & R. Schütte (Eds.), *Referenzmodellierung* (pp. 45–68). Heidelberg: Physica-Verlag HD.

RKW Berlin GmbH (Ed.) (2008). *Auszüge aus der Benchmarking-StudieQualitätsmanagement Berlin-Brandenburg 2008.* Berlin. Retrieved March 01, 2016, from http://www.benchmarkingforum.de/fileadmin/publikationen_buecher/Broschuere_Ergebnisse_QM-Studie.pdf.

Rosemann, M., & Schütte, R. (1997). Grundsätze ordnungsmäßiger Referenzmodellierung. In J. Becker, M. Rosemann, & R. Schütte (Eds.), *Entwicklungsstand und Entwicklungsperspektiven der Referenzmodellierung. Arbeitsberichte des Instituts für Wirtschaftsinformatik. Proceedings zur Veranstaltung vom 10.03.1997,* Vol. 52, pp. 16–33. Münster.

Schilling, A., & Werners, B. (2016). Optimal selection of IT security safeguards from an existing knowledge base. *European Journal of Operational Research, 248*(1), 318–327. Retrieved May 02, 2016.

Schreiner, M., Hess, T., & Benlian, A. (2015). *Gestaltungsorientierter Kern oder Tendenz zur Empirie?: Zur neueren methodischen Entwicklung der Wirtschaftsinformatik* (WIM). Ludwig-Maximilians-Universität München. Retrieved November 15, 2015, from http://www.ise.tu-darmstadt.de/media/ise/publikationen_3/AB_WI_Methoden_1_15.pdf.

Schütte, R. (1998). *Grundsätze ordnungsmäßiger Referenzmodellierung: Konstruktion konfigurations- und anpassungsorientierter Modelle.* Zugl.: Münster, Univ., Diss., 1997. *Neue betriebswirtschaftliche Forschung: Vol. 233.* Wiesbaden: Gabler.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action Design Research. *MIS Quarterly, 35*(1), 37–56.

Sowa, S., Tsinas, L., Lenz, H., & Gabriel, R. (2009). Integrated Information Security Risk Management – Merging Business and Process Focussed Approaches. In R. H. Hansen, D. Karagiannis, & H.-G. Fill (Eds.), *Business Services: Konzepte, Technologien, Anwendungen* (Vol. 1, pp. 327–336). Wien: Österreichische Computer Gesellschaft.

Stachowiak, H. (1973). *Allgemeine Modelltheorie [General Model Theory].* Wien, New York: Springer-Verlag.

Straub, D., & Ang, S. (2011). Rigor and Relevance in IS Research: Redefining the Debate and a Call for Future Research. *MIS Quarterly, 35*(1), iii–xi.

Thornburgh, T. (2004). Social engineering: The "Dark Art". In M. Whitman (Ed.), *Proceedings of the 1st annual conference on Information Security Curriculum Development* (pp. 133–135). New York, NY: ACM.

Venable, J. R. (2007). Relevance vs. Rigour or Relevance and Rigour? Contingence and Invariance in Standards for IS Research. *WIRTSCHAFTSINFORMATIK, 49*(5), 407–409.

Vom Brocke, J. (2003). *Referenzmodellierung: Gestaltung und Verteilung von Konstruktionsprozessen. Advances in information systems and management science: Bd. 4.* Berlin: Logos-Verl.

Wall, D. S. (2012). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal, 26*(2), 107–124.

Wilde, T., & Hess, T. (2007). Forschungsmethoden der Wirtschaftsinformatik. *WIRTSCHAFTSINFORMATIK, 49*(4), 280–287.

Winter, R. (2007). Relevance and Rigour – What are Acceptable Standards and How are they Influenced? *WIRTSCHAFTSINFORMATIK, 49*(5), 403–409.

Wissenschaftliche Kommission Wirtschaftsinformatik (WKWI) im Verband der Hochschullehrer für Betriebswirtschaft e.V. und Fachbereich Wirtschaftsinformatik (FB WI) in der Gesellschaft für Informatik e.V. (GI) (Ed.) (2011). *Profil der Wirtschaftsinformatik.* Retrieved December 08, 2015, from http://wi.vhb online.org/fileadmin/Kommissionen/WK_WI/Profil_WI/Profil_WI_final_ds26.pdf.

Wolf, M. R., & Altgen, J. (2013). *IT Service Management in der Region Aachen.* FH Aachen, Labor für IT Organisation & Management. Retrieved February 14, 2016, from http://itom.ac/files/download/34734ef6bd9a055.