Universidad
Carlos III de Madrid
www.uc3m.es

TESIS DOCTORAL

Maturity based approach for ISMS governance

Autor:

Knut Haufe

Directores:

Ricardo Colomo Palacios

Vladimir Stantchev

Tutor:

José María Álvarez Rodríguez

DEPARTAMENTO DE INFORMÁTICA

Leganés, Marzo 2017

Universidad
Carlos III de Madrid
www.uc3m.es

TESIS DOCTORAL

MATURITY BASED APPROACH FOR ISMS GOVERNANCE

Autor: *Knut Haufe*

Directores: **Ricardo Colomo Palacios y Vladimir Stantchev**

Firma del Tribunal Calificador:

Firma

Presidente: Antonio de Amescua Seco

Vocal: Rafael Valencia García

Secretario: Tomás San Feliú Gilabert

Calificación:

Leganés,

Contents

List of Figures

List of Tables

Acknowledgements

For the ancestors who paved the path before me and upon whose shoulders I stand.

I dedicate this thesis especially to my parents Manfred and Gundula and my grandmother Edith making my education possible.

I also dedicate this thesis to my wife Tina – writing this thesis would not have been possible without your constant support – and to my children Alexander and Helena: I know you will probably never read it, but I will do my best to encourage you to always learn.

I would like to express my deepest gratitude to my supervisors Ricardo Colomo-Palacios and Vladimir Stantchev for your support, collegiality and mentorship – and for constantly pushing me in the right direction.

Resumen

La seguridad de la información es un elemento integral del deber fiduciario. El propósito de la seguridad de la información es proteger los recursos de una organización, incluyendo en los mismos la información. La seguridad de la información es también un subconjunto de la gobernanza de TI y debe gestionarse dentro de un Sistema de Gestión de la Seguridad de la Información (por sus siglas en inglés ISMS). El elemento clave del funcionamiento de un ISMS son los procesos del ISMS.

La investigación actual se centra en aspectos económicos como el análisis de coste-beneficio de la inversión en seguridad de la información en relación a medidas individuales de protección de la información. De esta forma, los procesos del ISMS no están en el foco de la investigación actual. Así, todavía no existe un marco de proceso ISMS específico que diferencie claramente entre procesos ISMS y medidas de seguridad controladas por procesos ISMS, así como una descripción de procesos ISMS y su interacción. Para construir este marco, los procesos del ISMS, así como su nivel de madurez, deben estar alineados con la organización que los implanta así como con su misión. Tomando en consideración que las empresas presentan unos recursos limitados y que los recursos disponibles deben ser explotados de forma eficiente, no todos los procesos del ISMS deben ser establecidos y operados en el mismo nivel de madurez.

Teniendo en cuenta que la alineación con el negocio y la rentabilidad son aspectos importantes para el funcionamiento exitoso de un ISMS, las contribuciones a la investigación del tópico deben abordar tanto los procesos del ISMS como la determinación de su nivel de madurez objetivo. Por lo tanto, el objetivo general de esta tesis doctoral es encaminar a las organizaciones hacia la construcción de un ISMS transparente, así como evitar costos innecesarios de la gobernanza de la información aspecto que sigue siendo una dificultad para muchas organizaciones.

Esta tesis doctoral propone un marco de proceso ISMS basado en un conjunto de procesos acordados de ISMS en las normas vigentes existentes como la serie ISO 27000, COBIT e ITIL. Dentro del marco, se describen los procesos identificados y se especifica su interacción y las interfaces entre los mismos. Este marco ayuda a centrarse en el funcionamiento del ISMS en lugar de poner el foco en medidas y controles. Con esta aproximación, se fortalece el carácter sistémico del ISMS y la percepción de los roles relevantes del ISMS como un sistema de gestión que consiste en procesos. Para un uso eficiente del marco del proceso ISMS se propone un método para determinar el nivel de madurez individualmente necesario de los procesos del ISMS.

Abstract

Information security is an integral element of fiduciary duty. The purpose of information security is to protect an organization's valuable resources, such as information. Information security is also a subset of IT governance and must be managed within an Information Security Management System (ISMS). Key element of the operation of an ISMS are ISMS processes.

Current research focuses on economics and cost benefit analysis of information security investment regarding single measures protecting information. ISMS processes are not in the focus of current research. Actually a specific ISMS process framework which clearly differentiates between ISMS processes and security measures controlled by ISMS processes as well as a description of ISMS processes and their interaction does not exist yet. ISMS processes as well as their maturity level need to be aligned to the implementing organization and their mission to be cost-effective. Considering limited resources as well as ensuring an efficient use of those resources not every ISMS process should be established and operated at the same level of maturity.

Taking into account that business alignment and cost-effectiveness are important for the successful operation of an ISMS, research contributions must address both problems – ISMS processes as well as the determination their target maturity level. Therefore the overall objective of this doctoral thesis is to make the appropriateness of an ISMS transparent as well as to avoid unnecessary costs of information governance which is still a major issue/problem for many organizations.

This doctoral thesis aims to fill this research gap by proposing an ISMS process framework, based on a set of agreed upon ISMS processes in existing applicable standards like ISO 27000 series, COBIT and ITIL. Within the framework, identified processes are described and their interaction and interfaces are specified. This framework helps to focus on the operation of the ISMS instead of focusing on measures and controls. By this the systemic character of the ISMS and the perception of relevant roles of the ISMS as a management system consisting of processes is strengthened. For an efficient use of the ISMS process framework a method to determine the individually necessary maturity level of the ISMS processes is proposed.

Part I – Introduction and Objectives

1 Introduction

1.1 Introduction

Information security is an integral element of fiduciary duty. The purpose of information security is to protect an organization's valuable resources, such as information (Peltier, 2013). Information security is also a subset of IT governance (Calder, 2009).

According to Fenz and Ekelhart (2009) the fundamental concepts and relationships of information security are depicted in Figure 1 – Fundamental concepts and relationships of information security.

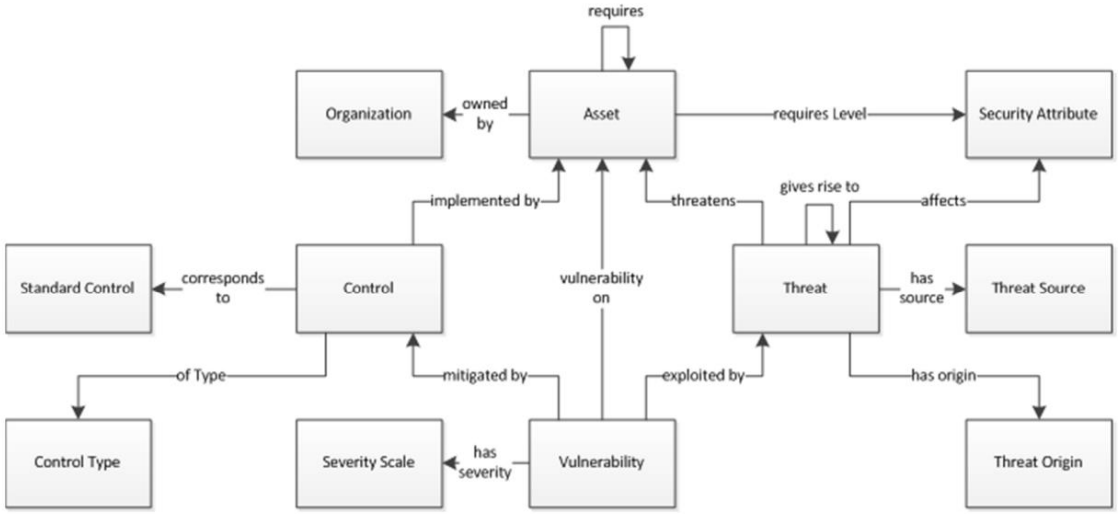

Figure 1 – Fundamental concepts and relationships of information security

In relevant standards and frameworks as well as in the literature the continuous increasing dependency of nearly all organizations on appropriate secure information processing was stated practically in the last years (Alvaro, 2009, p. 214; German Federal Office for Information Security, 2008, p. 5; Kittel, Koerting, & Schött, 2006, p. 18; Martins & Elofe, 2002; Sambamurthy, Bharadwaj, & Grover, 2003).

Standards for the management of information security and collections of best practice measures were developed and established in the literature, e.g. (International Organization for Standardization and International Electrotechnical Commission, n.d.), (International Organization for Standardization and International Electrotechnical Commission, 2013a), (International Organization for Standardization and International Electrotechnical Commission, 2013b), (German Federal Office for Information Security, 2008), (German Federal Office for Information Security, 2013).

Beside national standards like NIST SP 800 series in the US (U.S. Department of Commerce - National Institute of Standards and Technology, n.d.) or the IT security guidelines from the Federal Office for Information security in Germany (German Federal Office for Information Security, 2013) the most important standards for the development and operation of an information security management system (hereinafter referred to as "ISMS") are the ISO 270xx, ITIL and COBIT (Stoll, 2014). The same standards were identified as most used standards for IT governance and IT management followed by CMM and CMMI, PRINCE2 and PMBOK in an ISACA study (Information Systems Audit and Control Association, 2008, p. 26). Also in the work of Susanto, Almunawar and Tuan (2011), ISO 270xx is recognized as the most widely accepted information security standard next to standards as COBIT and ITIL. Some authors are also recognizing ISO 38500 as a relevant standard. This standard is not used in this thesis because ISO 38500 contains a process assessment model and no information about ISMS processes itself.

1.2 Significance of the thesis

Frequent obstacles regarding the implementation of an ISMS and of the security measures controlled by ISMS-processes are the continuous raising number of those measures and their complexity.

At first glance standards like ISO 27001/BSI 100-1 and ISO 27002 contain a manageable amount of security measures. But those generic measures need to be individually adapted and substantiated by the user of the standards during their individual planning and operation of the ISMS. So, from a security perspective necessary processes and measures need to be planned and implemented adequately. This is done and managed by the chief information security officer (CISO) with limited resources (Bodin, Gordon, & Loeb, 2005). Considering limited resources as well as ensuring an efficient use of those resources not every ISMS process should be established and operated at the same level of maturity (Information Systems Audit and Control Association, 2008, p. 8).

Typical departments including risk management, legal, audit, compliance, privacy, business continuity, quality control, facilities, human resources, IT security, information security and physical security are all engaged in activities that have a bearing on, or are related to, security. However, their activities tend to be viewed as silos, they are typically not connected and they collectively may consume more than a quarter of organizational resources. Integration of these activities into a model that makes explicit the interrelationships will enable a more cost-effective security (Information Systems Audit and Control Association, 2009, p. 11). The ITIL framework (Office of Government Commerce, 2007a) integrates the idea to charge costs for IT-services to the functional units which use the IT-services. Considering this idea in the information security management it sounds obvious to charge costs for information security measures to the functional units which demand those measures. To realize this a clear differentiation between ISMS processes which are financed by the budget of the CISO and other security measures which are financed by other cost centers should be made. As a result, information security costs are made transparent and can be better managed.

Actually, a specific process framework for security management, which clearly differentiates between ISMS processes and the security measures controlled by ISMS-processes, does not exist. Furthermore, a detailed description of ISMS processes and their interaction as well as the interface with other management processes – as already identified in (Eloff & Eloff, 2005) – does not exist.

The missing differentiation of ISMS processes and security measures as well as the missing ISMS process framework are still a problem for many organizations because information security management is a complex issue (Baskerville, Spagnoletti, & Kim, 2014). Current research focus on economics and cost benefit analysis of information security investment regarding single measures protecting information (Gordon & Loeb, 2002; Gordon & Loeb, 2006; Pieters, Probst, Lukszo, & Montoya, 2014). Information security standards focus on the existence of processes, not on their content (Siponen, 2006a). The ISMS and the ISMS processes itself are not focused in current research.

Measures as well as ISMS processes must be aligned to the processes and objectives of the organization and their mission (Fakhri, Fahimah & Ibrahim, 2015). To determine the necessary and appropriate measures as well as to align the ISMS processes to the business needs, knowledge of the mission of the organization is needed. Taking into account that business alignment (Fakhri et al., 2015) and cost-effectiveness (Peltier, 2013) are important for the successful operation of an ISMS, research contributions must address both problems by allowing the simplification of the identification of necessary and appropriate security measures as well as ISMS processes as core elements of every ISMS.

To sum up, the particular problems from different viewpoints are:

- From the customer perspective: The implementation of an ISMS is complex, challenging and often it is not clear, what an ISMS is and what are specific measures outside the ISMS. The ISMS is represented by interacting ISMS processes. No standardized process framework is available for the information security professionals which results in unnecessary costs for designing and implementing an ISMS.
- From the scientific viewpoint: Current research does not focus on ISMS processes. It is also not clear what processes are ISMS processes. Considering limited resources as well as ensuring an efficient use of those resources not every ISMS process should be established and operated at the same level of maturity (Information Systems Audit and Control Association, 2008, p. 8). A method to identify the necessary maturity level of those processes does also not exist, but would solve the problem of inefficient resource usage.

Over the last few years, cost benefit discussions have influenced information security practice (Whitman & Mattord, 2013, p. 329). The value of information must justify protection costs (Peltier, 2016). Adjustment and cost-effectiveness are key elements of a successful ISMS (Peltier, 2013).

Therefore the overall objective of this doctoral thesis is to make the appropriateness of an ISMS transparent as well as to avoid unnecessary costs of information governance which is still a major issue/problem for many organizations (Coulson, Zhu, Miyuan, & Rohm, 2015) and unsolved from the scientific viewpoint (Gordon & Loeb, 2002, Gordon & Loeb, 2006, Pieters et al., 2014).

1.3 Research objectives

Research on the various security issues regarding information security has been done in the past. Current research focus on economics and cost benefit analysis of information security investment regarding single measures protecting information but not focusing at the ISMS and the ISMS processes itself (Gordon & Loeb, 2002, Gordon & Loeb, 2006, Pieters et al., 2014).

The classic PDCA cycle explains mainly the big picture how to plan, implement, check and improve an ISMS (International Organization for Standardization and International Electrotechnical Commission, 2013a). But is does not explain ISMS core processes and their interaction at a detailed basis. Also while auditing an ISMS – for example in certification processes – the two core questions which need to be answered by the auditor are (International Organization for Standardization, 2011, Chapter 6.4.8; International Organization for Standardization and International Electrotechnical Commission, 2011b, Chapter 9.2.3.2.1):

1) Is the ISMS running/operative?
2) Is the ISMS adequate regarding the requirements and objectives of the institution?

To answer the first question, the core processes of the ISMS need to be checked. To answer the second question, the maturity level of those core processes need to be checked if they are implemented at an appropriate maturity level.

The most relevant contribution of this doctoral thesis will be the provision of a framework of ISMS core processes (processes are differentiated in core, management and supporting processes (International Organization for Standardization and International Electrotechnical Commission, 2005) – see also chapter 2.2) as core elements of every ISMS as well as a method to determine the necessary maturity level of the processes. By considering a maturity level model for ISMS processes combined with an approach for the determination of the necessary maturity level the appropriateness of an ISMS will be made transparent as well as unnecessary costs of information governance will be avoided.

To achieve this objective the following sub-objectives are defined:

1. ***Objective – Develop an ISMS core process framework***

First objective of this thesis is to derive a generic state of the art model of core processes of an ISMS from a set of standards, which will be determined.

2. ***Objective – Select or modify an existing maturity level model for the use with the ISMS core process framework***

According to Lessing (2008), an organization with full information security maturity, continuous assessment of maturity concerning information security, is able to respond to any information security related circumstances in an appropriate manner. But considering limited resources as well as ensuring an efficient use of those resources, not every ISMS process should be established and operated at the same level of maturity (Information Systems Audit and Control Association, 2008, p. 8).

So, for the usage with the developed ISMS core process framework, an appropriate maturity level model needs to be selected from the established standards or an existing maturity level model needs to be modified for the use with the ISMS core process framework.

3. Objective – Develop or identify a method to determine the necessary maturity level of ISMS core processes

For an efficient use of the ISMS process framework and the maturity level model a method to determine the necessary maturity level must be identified or developed.

4. Objective – find a proper method to evaluate and validate assumptions with experts

To accomplish the aforementioned objectives, assumptions must be made while performing the research. These assumptions must be evaluated and validated with experts. A proper method for this evaluation and validation is necessary to substantiate the assumptions and, as a result of this, also the research results.

1.3.1 Research questions

The objectives of this doctoral work are focused on the development of a generally applicable ISMS core process framework as a prototype for an ISMS as well as a tailoring methodology to ensure the appropriateness of the individual implementations of the ISMS. Therefore this arises three main research questions (MRQ), which are detailed as follows:

- MRQ1: Which elements does the agreed ISMS core process framework consists of?
  - MRQ1-1: What are criteria to identify processes and ISMS core processes?
  - MRQ1-2: Are there defined ISMS processes existing in established standards?
    - MRQ1-2-a: Which are the possible ISMS core processes defined in established standards?
    - MRQ1-2-b: To what extent are the processes described in the ISO 27001, ITIL and COBIT models related?
  - MRQ1-3: Are there defined ISMS processes existing in the latest ISMS process framework research?
  - MRQ1-4: What is the agreed basis of ISMS processes in existing standards and in the latest ISMS process research work?
- MRQ2: Are there maturity level models and methods applicable for information security management processes existent?
  - MRQ2-1: What are criteria for the applicability of maturity models within ISMS?
  - MRQ2-2: Are maturity models already used within ISMS?

  - MRQ2-3: What is the most appropriate maturity model for the use within ISMS?
- MRQ3: Which method should be used to determine the necessary maturity level of ISMS core processes?
  - MRQ3-1: What methods are used for the determination of the necessary maturity level?
  - MRQ3-2: Which method is most suitable to determine the necessary maturity level of ISMS processes?

Answering MRQ1 and the sub-research questions of MRQ1 will result in reaching objective 1 – Develop an ISMS core process framework.

Answering MRQ2 and the sub-research questions of MRQ2 will result in reaching objective 2 – Select or modify an existing maturity level model for the use with the ISMS core process framework.

Answering MRQ3 and the sub-research questions of MRQ3 will finally result in reaching the objective 3 – Identify or develop a method to determine the necessary maturity level of ISMS core processes. This dependencies are displayed in Figure 2 – General dependencies of objectives and research questions of this thesis.

Objective 4 must be reached inclusively while answering the research questions regarding the other objectives. Therefore objective 4 is not shown separately in Figure 2 – General dependencies of objectives and research questions of this thesis.

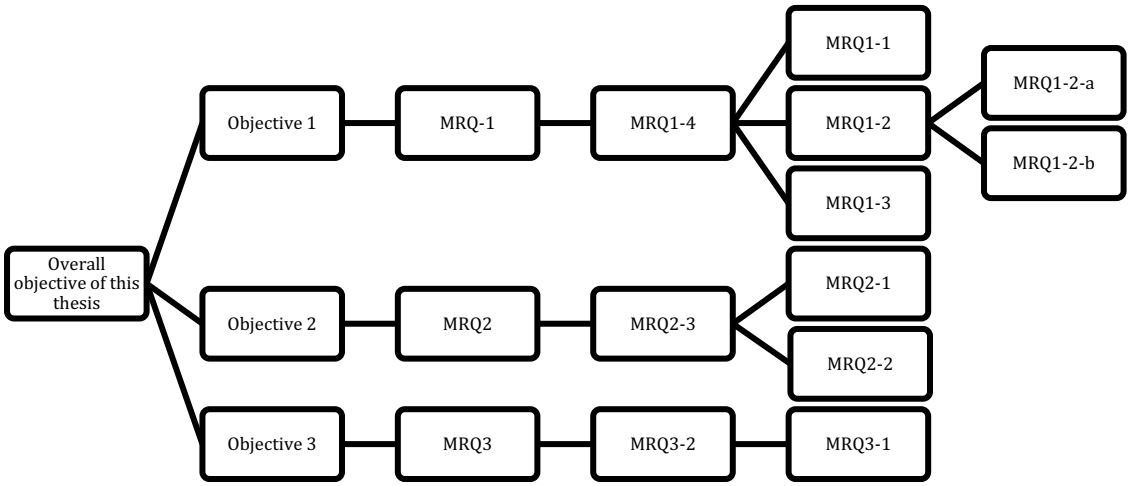

Figure 2 – General dependencies of objectives and research questions of this thesis

1.3.2 Hypothesis

Taking into account the research questions the following hypothesis is formulated aimed to be validated in this doctoral thesis:

If there exist definitions of ISMS processes in the existing and relevant standards or in the latest research and if there exist maturity level models and methods applicable for information security, then this can be combined to a generally applicable ISMS core process framework as well as a methodology to tailor the processes and their maturity level to the requirements of the implementing organizations resulting in a transparent appropriateness of the ISMS.

1.4 Solution approach

In the following, the approach to achieve the research objectives and the foresee results of the thesis will be described.

1.4.1 Analysis

To achieve the research objectives the following analysis activities will be conducted:

1. Identification of ISMS core processes

MRQ1 asks for agreed elements of an ISMS core process framework. For this thesis an element is agreed, if it is mentioned in one of the three most accepted standards for information security (ISO 270xx, ITIL or COBIT) or it is mentioned at least more than once in the latest ISMS process research work. Some authors are also recognizing ISO 38500 as a relevant standard. This standard is not used in this thesis because ISO 38500 contains a process assessment model and no information about ISMS processes itself.

To answer MRQ1: "Of which elements does the agreed ISMS core process framework consists?" the following research tasks will be performed:

- Task 1 [Research state of the art publications and conduct a study]: As a prerequisite, criteria for the identification of processes as well as for the categorization of processes as ISMS core process will be developed by analyzing relevant state of the art publications to answer MRQ1-1: "What are criteria to identify processes and ISMS core processes?" Those criteria will be evaluated and justified or dismissed within a study. The results of this task are documented in chapter 5.1
- Task 2 [Apply the process criteria to the relevant standards]: The identified process criteria will be applied to the frameworks and standards to identify mentioned processes and to answer MRQ1-2-a: "Which are the possible ISMS core processes defined in established standards?" The following frameworks and standards will be analyzed:
  - ISO 270xx, specified in (International Organization for Standardization and International Electrotechnical Commission, 2013a), (International Organization for Standardization and International Electrotechnical Commission, 2013b)

  - Control Objectives for Information and related Technology (COBIT), specified in (Information Systems Audit and Control Association, n.d.)
  - IT Infrastructure Library (ITIL), specified in (Office of Government Commerce, 2007a, 2007b, 2007c, 2007d, 2007e, 2007f)

  The results of this task are documented in chapter 5.3
- Task 3 [Conduct a mapping]: To answer MRQ1-2-b: To what extent are the processes described in the ISO 27001, ITIL and COBIT models related?" a mapping study is conducted.
  The results of this task are documented in chapter 5.3
- Task 4 [Apply ISMS process criteria to possible ISMS processes] – To answer the research question MRQ1-2: "Are there defined ISMS processes existing in established standards?" the results of tasks 1 to 3 are analyzed taking into account the criteria for ISMS core processes. For this the frameworks and standards will be analyzed and compared on a detailed basis regarding the description of ISMS core processes. Similarities will be identified and discrepancies will be discussed. For each ISMS core process a process chart as well as a process profile will be developed, containing the following elements:
  - Process name
  - Process categorization
  - Brief description
  - Objectives/purposes
  - Input/output (interfaces)
  - Activities/functions
  - Metrics
  - Owner, manager and actors

  The results of this task are documented in chapters 5.5.
- Task 5 [Conduct a systematic literature review]: To answer the research question MRQ1-3: "Are there defined ISMS processes existing in the latest ISMS process framework research?" a systematic literature analysis (SLR) will be conducted.
  The results of this task are documented in chapter 5.3

2. Analysis and selection of a maturity level model

For the implementation of the ISMS core processes an appropriate maturity level model needs to be identified and selected. An easy to use method for the determination of the necessary maturity level for the ISMS processes needs to be identified or developed.

To achieve the second research objective – Develop, select or modify an existing maturity level model for the use with the ISMS core process framework – the following tasks will be conducted:

- Task 6 [Conduct a systematic literature review]: As a prerequisite, criteria for the applicability of a maturity level model for the use within an ISMS will be developed within an systematic literature analysis to answer the research question MRQ2-1 "What are criteria for the applicability of maturity models within ISMS?"
  The results of this task are documented in chapter 6

- Task 7 [Conduct a systematic literature review]: A systematic literature review will be conducted to answer the research question MRQ2-2: Are maturity models already used within ISMS? The following frameworks and standards will be analyzed:
  - CMMI (CMMI Product Team, 2010a, 2010b, 2010c),
  - ISO/IEC 15504, also known as SPICE (International Organization for Standardization and International Electrotechnical Commission, 2004a),
  - O-ISM^3 (Canal, n.d.) and
  - ISO/IEC 21827, also known as SSE-CMM (*Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)*, 2008).

  The results of this task are documented in chapter 6
- Task 8 [Apply criteria of task 1 to relevant maturity level models]: The identified criteria for the applicability of a maturity level model for the use within an ISMS will be applied to the relevant maturity level models. The results will be the basis for the selection of an appropriate maturity level model to answer the research question MRQ2-3: "What is the most appropriate maturity model for the use within an ISMS?".
  The results of this task are documented in chapter 6

3. Analysis and selection of methods for the determination of the necessary maturity level

To answer MRQ3-1: "What methods are used for the determination of the necessary maturity level?" the following task will be conducted:

- Task 9 [Conduct a systematic literature review]: A systematic literature review will be conducted to identify and categorize all relevant research papers related to methods for the determination of the necessary maturity level of processes or in particular ISMS core processes. The result of this task is documented in chapter 7.

1.4.2 Conception

The following tasks will be performed to answer the research questions MRQ1-4, MRQ2-3 and MRQ3-2.

- Task 10 [Conception]: To answer the research question MRQ1-4: "What is the agreed basis of ISMS processes in existing standards and in the latest ISMS process research work?" the results from MRQ1-2 to MRQ1-3 will be used to develop an ISMS core process framework. A first draft of the ISMS core process model will be developed and refined later with the results from an expert study and with the results from the pilot application. This will finally result in **achieving the first research objective** – develop an ISMS core process framework by answering research question MRQ1 "Of which elements does the agreed ISMS core process framework consists?"
  The result of this task is documented in chapter 0

- Task 11 [Conception]: The criteria for the applicability of a maturity level model for the use within an ISMS (MRQ-2-1) will be applied to the maturity level models. This and the answer to research question MRQ2-2 will be the basis for the selection of an appropriate maturity level model to answer the research question MRQ2-3 "What is the most appropriate maturity model for the use within an ISMS?" and **achieve the second research objective**.
  The result of this task is documented in chapter 6
- Task 12 [Conception]: Based on the result of the systematic literature review (SLR) to identify and categorize all relevant research papers related to methods for the determination of the necessary maturity level of processes an existing method will be selected or modified (conception) for the use with ISMS processes or a new method will be developed (conception) to answer MRQ3-2: "Which method is most suitable to determine the necessary maturity level of ISMS processes?" and to **achieve the third objective** – Develop or identify a method to determine the necessary maturity level of ISMS core processes.
  The result of this task is documented in chapter 7

1.4.3 Pilot application and expert consultation

Regarding the pilot application and expert consultation the following tasks will be performed:

- Task 13 [expert consultation study]: Results of the precedent steps will be checked and validated or dismissed in an expert consultation study (ISMS auditors, security manager and CEOs).
  The results of this task are documented in chapter 0
- Task 14 [pilot application]: A pilot application regarding a planning and implementation of an ISMS will be conducted.
  The results of this task are documented in chapter 8.2.4

1.4.4 Evaluation

Regarding the evaluation the following tasks will be performed:

- Task 15 [Discussion]: Results from the pilot application and the expert consultation will be discussed to identified optimization potentials
  The results of this task are documented in chapter 8.2.4
- Task 16 [Optimization of the results]: Results of the expert consultation as well as practical experience of the pilot application will be used to optimize the results.
  The results of this task are documented in chapter 8.4.

1.4.5 Conclusion

Results of this thesis will be summarized and possible further research will be discussed.

1.5 Research methodology

The research method for this thesis will follow the design-science paradigm for Information Systems research (Hevner & Chatterjee, 2010) and their fundamental principle of design-science research "knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact".

"Design science research is a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artifacts, thereby contributing new knowledge to the body of scientific evidence. The designed artifacts are both useful and fundamental in understanding that problem" (Hevner & Chatterjee, 2010)

In the work of Hevner and Chatterjee (2010) the following seven guidelines are described:

Guideline 1: Design as an artifact

"Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation".

The author proposes to identify and describe a framework for ISMS processes as well as a method for the determination of the necessary maturity level with the aims to make the appropriateness of an ISMS transparent as well as to avoid unnecessary costs of information governance.

Guideline 2: Problem relevance

"The objective of design-science research is to develop technology-based solutions to important and relevant business problems".

Adjustment and cost-effectiveness are key elements of a successful ISMS (Peltier, 2013). A detailed framework of ISMS processes (input, output, interfaces) and their interaction at an activity level helps to ensure an appropriate interaction of the ISMS processes. By considering a maturity level model for ISMS processes combined with an approach for the determination of the necessary maturity level the appropriateness of an ISMS can be made transparent as well as unnecessary costs of information governance can be avoided.

Guideline 3: Design evaluation

"The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods".

The design of the framework of ISMS processes and the approach for the determination of the necessary maturity levels will be verified in an expert consultation (ISMS auditors, security manager and CEOs). Furthermore a pilot application regarding a planning and implementation of an ISMS will be conducted. Results of the expert consultation as well as practical experience of the pilot application will be used to optimize the results.

Guideline 4: Research contributions

"Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies".

The novelty of this research work lies in the clear differentiation between ISMS processes which are financed by the budget of the CISO and other security measures which are financed by other cost centers as well as the integration of a maturity based approach in the resulting ISMS process framework. The main research contributions are focused on filling the gap in the cost effectiveness and adequacy discussion which mainly focusses on specific measures and not ISMS processes itself.

Guideline 5: Research rigor

"Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact".

The proposed ISMS process framework and the maturity based approach will be developed under consideration, analysis and modification of existing standards and with the aim of proposing new standards if necessary. The rigorous methods for the evaluation will be based on a two steps approach: an survey followed by expert consultation meetings considering latest research in rigorous use of expert knowledge like (Drescher et al., 2013).

Guideline 6: Design as a search process

"The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment".

The design of the ISMS process framework as well as the maturity level approach will be undertaken incrementally and iteratively by considering new research work and expert knowledge as well as established standards and practical experience of the pilot application.

Guideline 7: Communication of research

"Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences".

This work is intended to be distributed on scientific journals, international conferences and book chapters, as well as published by the Universidad Carlos III de Madrid in partial fulfilment of the requirements for the PhD programme in "Ciencia y Tecnología Informática".

1.6 Structure of the thesis

To verify or dismiss the hypothesis – "If there exist definitions of ISMS processes in the existing and relevant standards or in the latest research and if there exist maturity level models and methods applicable for information security, then this can be combined to a generally applicable ISMS core process framework as well as a methodology to tailor the processes and their maturity level to the requirements of the implementing organizations resulting in a transparent appropriateness of the ISMS." – this thesis is divided into five main sections:

1. Introduction and objectives,
2. Background,
3. Contribution,
4. Evaluation and verification,
5. Conclusions.

The overall objective of this thesis – the development of a holistic framework of ISMS core processes as core elements of every ISMS as well as a method to determine the necessary maturity level of the processes to make the appropriateness of an ISMS transparent and to avoid unnecessary costs of information governance – is divided into a structure of research objectives and research questions as shown in Figure 2 – General dependencies of objectives and research questions of this thesis.

A roadmap of the structure of this thesis as well as the link between the structure and the research objectives and research questions is given in Figure 3 – Structure of the thesis.

The introduction part describes the research problem and objectives, gives an insight into the solution approach as well as the research methodology of this research work.

The background reviews the state-of-the-art in the field of management systems, business process management, information security management and process maturity. It consists of three chapters that cover the backbone of technologies and their fields of knowledge.

The contribution part details the research contribution of this thesis and provides a foundation for the remaining sections. The evaluation part focuses on proving that the contribution outcomes meet the research objectives stated herein.

And finally, the conclusion section gives a summary and outlook of the thesis by highlighting the findings, the achievements, and specifying future lines of work.

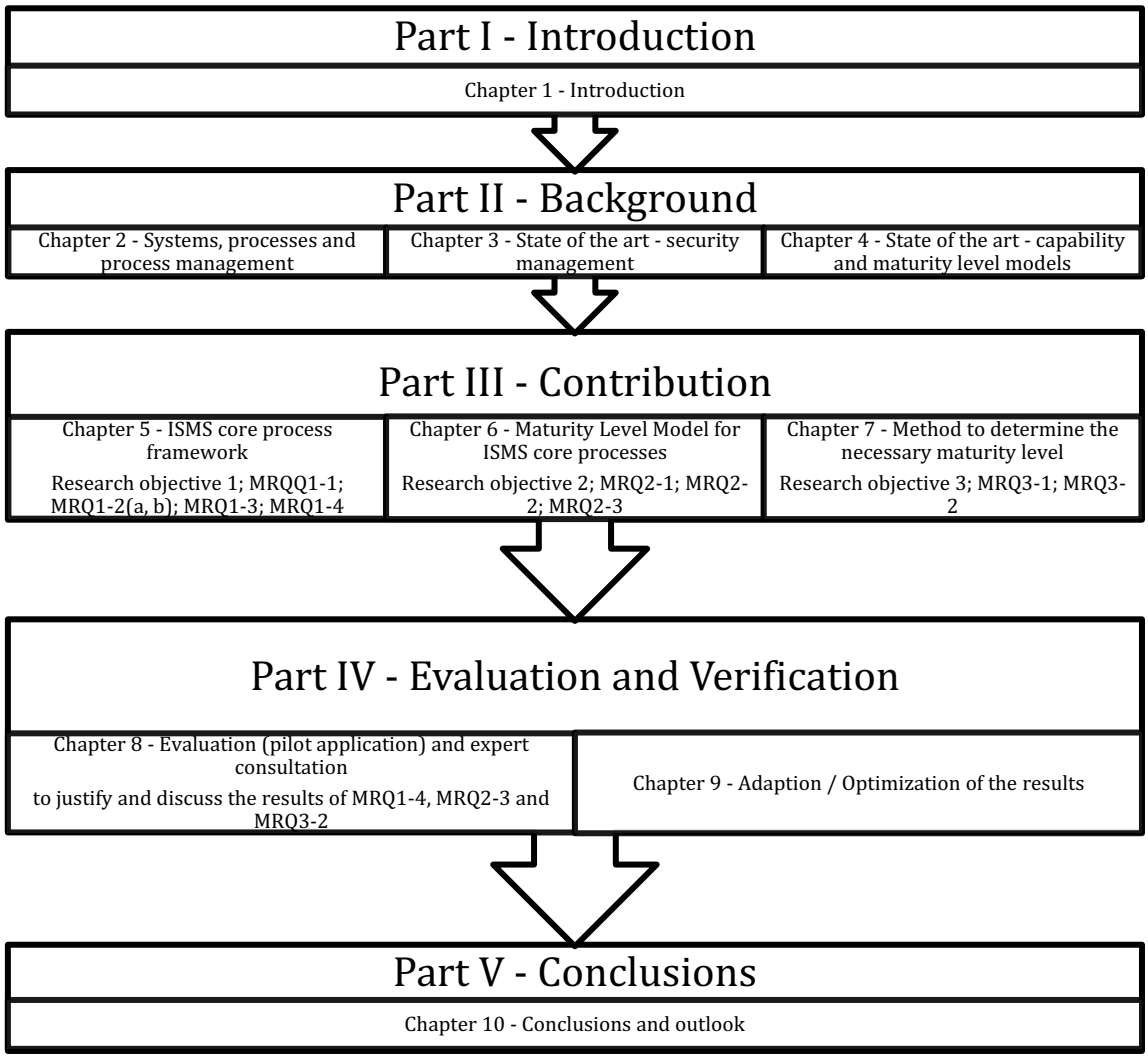

Figure 3 – Structure of the thesis

Chapter 1 – Introduction

This chapter includes an overview of the research work by describing the research problem and research goals as well as the solution approach and research methodology.

Chapter 2 – Systems, processes and process management

In this chapter an overview is given of key elements and disciplines related with this thesis. Those elements and disciplines are systems, processes and process management. Special attention is payed to methods for the identification and assessment of existing processes as this is a necessary method for this thesis.

Chapter 3 – State of the art - security management

In this chapter an overview of relevant and actual security management standards is given. Those standards are the ISO 27000 series, ITIL and COBIT. ISO 38500 is not used in

this thesis because ISO 38500 contains a process assessment model and no information about ISMS processes itself. On the basis of those standards possible ISMS core processes will be identified later in chapter 5 to answer MRQ1-2, MRQ1-3 and MRQ1-4.

Chapter 4 – State of the art - capability and maturity level models

In this chapter an overview of relevant and actual capability and maturity level models is given. Those standards are CMMI (CMMI Product Team, 2010a, 2010b, 2010c), ISO/IEC 15504, also known as SPICE (International Organization for Standardization and International Electrotechnical Commission, 2004a), O-ISM^3 (Canal, n.d.) and ISO/IEC 21827, also known as SSE-CMM (*Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)*, 2008). On the basis of those standards an appropriate maturity level model for ISMS core processes is chosen or later developed (see chapter 7).

Chapter 5 – ISMS core process framework

This chapter contains in a first part criteria for ISMS core processes (answering MRQ1-1), which is a prerequisite to answer MRQ1-2-a, MRQ1-2-b, MRQ1-3 and MRQ1-4. In this chapter also the results of a study are included and discussed regarding the identified criteria for ISMS core processes. The objective of this study was to verify or dismiss the identified criteria for ISMS core processes.

The second part of this chapter contains an analysis of the most relevant security management standards regarding mentioned ISMS processes to answer the main research question MRQ1-2-a: “Which are the possible ISMS core processes defined in established standards?” and a mapping study to answer the MRQ1-2-b: “To what extent are the processes described in the ISO 27001, ITIL and COBIT models related?”

In the third part of this chapter the ISMS core process criteria are applied to the possible ISMS core processes to discuss if the process is an ISMS core process.

In the fourth part of this chapter a systematic literature review is documented to answer the MRQ1-3: “Are there defined ISMS processes existing in the latest ISMS process framework research?”

The result of this discussion is an ISMS core process framework which is described in the fifth part of this chapter and will answer MRQ1-4 “What is the agreed basis of ISMS processes in existing standards and in the latest ISMS process research work?”

Chapter 6 – Maturity Level Model for ISMS core processes

As a prerequisite, criteria for the applicability of a maturity level model for the use within an ISMS will be developed within an systematic literature analysis to answer the research question MRQ2-1 ”What are criteria for the applicability of maturity models within ISMS?”

In this chapter also the results of a systematic literature review will be presented to answer the research question MRQ2-2 “Are maturity models already used within ISMS?”.

The identified criteria for the applicability of a maturity level model for the use within an ISMS will be applied to the relevant maturity level models. The results will be the basis for the selection of an appropriate maturity level model to answer the research question MRQ2-3 “What is the most appropriate maturity model for the use within an ISMS?”.

Chapter 7 – Method to determine the necessary maturity level

In this chapter the results of a systematic literature review will be presented to answer the research question MRQ3-1: What methods are used for the determination of the necessary maturity level?

Based on this results a method for the identification of the necessary maturity level of an ISMS core process will be chosen, modified or developed and proposed to answer MRQ3-2 “Which method is most suitable to determine the necessary maturity level of ISMS processes?”. The selection, modification or development of the method is the second key element of the contribution part.

Chapter 8 – Verification and Evaluation

In this chapter the results of an expert consultation are described. The expert consultation is conducted to review the identified processes and to verify if the identified ISMS core processes are the most relevant, correct and complete. So the results of this study verify or dismiss the results of MRQ1-4, which is discussed in chapter 0.

This chapter also contains a description of the pilot application of the ISMS core process framework to evaluate the ISMS core process framework as well as the method to identify the necessary maturity level of the ISMS core processes within a real life implementation in a medium sized government organization. The objective of the pilot application is to verify or dismiss the results of MRQ1-4, MRQ2-3 and MRQ3-1

Chapter 9 – Adaption of the framework after verification and evaluation

Results from the expert consultation as well as the pilot application are discussed and the ISMS core process framework as well as the method to identify the necessary maturity level of the ISMS core processes are optimized.

Chapter 10 – Summary and outlook

This chapter contains a summary of the thesis and the results of the research work. Furthermore the outcomes of the research are discussed regarding if they meet the research objectives. Also results and benefits from the research work will be discussed and limitations as well as potential future work will be identified to further improve the results of the thesis and to identify additional areas to explore in the future.

The link between the structure of this thesis and the research objectives and research questions is given in Figure 4– Dependencies of objectives and research questions related to the structure of this thesis.

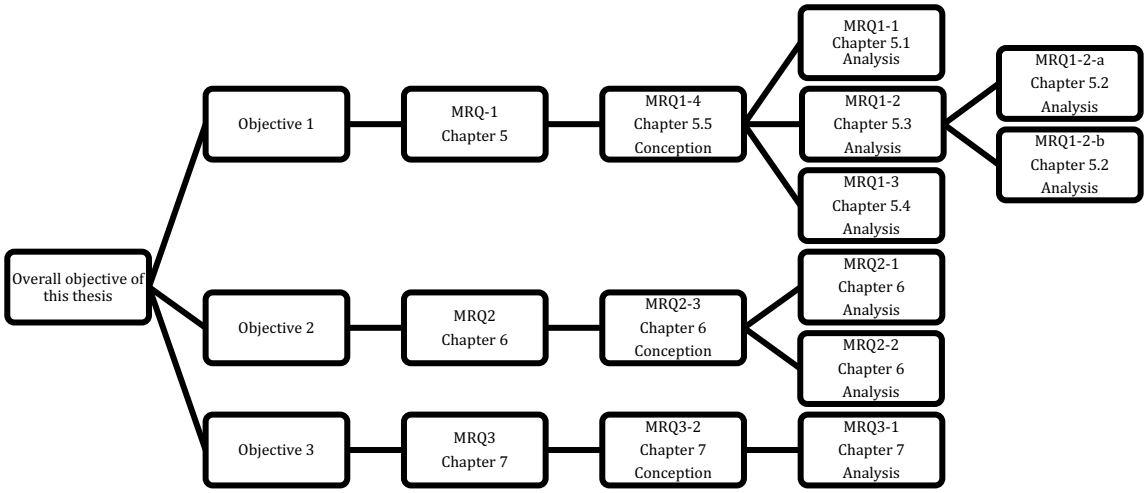

Figure 4 – Dependencies of objectives and research questions related to the structure of this thesis

Part II – Background

2 Systems, processes and process management

In this chapter an overview is given of key elements and disciplines related with this thesis. Those elements and disciplines are systems, processes and process management. Special attention is payed to methods for the identification and assessment of existing processes as this is a necessary method for this thesis. This chapter also focuses on criteria for ISMS core processes (answering MRQ1-1), which is a prerequisite to answer MRQ1-2-a, MRQ1-2-b, MRQ1-3 and MRQ1-4. In this chapter also the results of a study are included and discussed regarding the identified criteria for ISMS core processes. The objective of this study was to verify or dismiss the identified criteria for ISMS core processes.

2.1 Systems

According to (Information Systems Audit and Control Association, 2009, p. 8) "a system is an organized collection of parts (or subsystems) that are highly integrated to accomplish an overall goal. The system has various inputs, which go through certain processes to produce certain outputs, which together accomplish the overall desired goal for the system – The essence of systems theory is that a system needs to be viewed holistically—not merely as a sum of its parts—to be accurately understood. A holistic approach examines the system as a complete functioning unit. Utilizing a systems thinking approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, Systems thinking should be seen as a long-term exercise that will ultimately aid the enterprise in achieving business goals."

2.2 Processes

Organizations need to identify and manage many activities in order to function effectively and efficiently. Any activity using resources needs to be managed to enable the transformation of inputs into outputs using a set of interrelated or interacting activities – this is also known as a process (International Organization for Standardization and International Electrotechnical Commission, 2014, p. 8). In other words, a process is a set of interrelated or interacting activities which transforms inputs into outputs (International Organization for Standardization and International Electrotechnical Commission, 2005) – the objective of the process. A business process is described as a procedure relevant for adding value to an organization (Scheer & Nüttgens, 2000).

The term process originates from the Latin term "procedure" = going ahead, going forward. Processes can be part of other processes or contain other processes or initiate other processes. Unlike projects processes can be performed repeatedly. Processes are often performed interdepartmentally and are part of the operational structure of an organization. Processes are differentiated in core, management and supporting processes (International Organization for Standardization and International Electrotechnical Commission, 2005):

- Core processes deliver apparent and direct customer value and are derived from the core competencies of an organization.
- Management processes define the objectives of the organization as well as control and monitor the achievement of the objectives at the level of the core processes and the overall organization. They contain project-, quality-, security- and risk management as well as strategic planning.
- Supporting processes provide and manage necessary resources without delivering direct customer value. They support core and management processes. Typical supporting processes are human resources, financial management and IT management.

Functions are the smallest part of a process and describe with the use of activities a chronological and logical sequence. The sequence of activities in a function is defined by a logical combination where not defined by input-output-relations. The execution of a function is carried out by a function owner – which is a role or an organizational unit – in a short time frame. Functions are normally reusable and appear often several times at different places – for example quality assurance and approval. After a function is carried out an event occurred or an output is produced. Normally, a function contains three to ten activities.

Roles are sets of clustered rights and obligations. Roles are assigned to natural people – individuals or groups. Organizational units are legal entities or divisions of an organization. Functional ownership is primary assigned to roles instead of organizational units to prevent changes in the process documentation if the organizational structure changes. For every process or sub-process a process owner, process manager and process actors can be defined:

- Process owner are accountable for reaching the process objectives. They define measures for the performance – key performance indicators (KPI) – and the achievement of the process objectives – key goal indicators (KGI). Process owners delegate the execution of the process to the process manager. The process owner is also responsible for the design of the process (Information Systems Audit and Control Association, n.d.-d, p. 128)
- Process manager are responsible to manage and improve the process at an operational level, manage the process actors as well as measure and report the KPI/KGI.
- Process actors execute the process or parts of them (as function owners).

2.3 Process management

Process management is an approach to managing organizations and is focused on using business processes as a significant contributor to achieving an organization's objectives through the improvement, ongoing performance management and governance of essential processes (Jeston & Nelis, 2014). Furthermore, process governance is one of the critical success factors of a process-focused and high performance management organization (Jeston & Nelis, 2014).

Business process management can also be viewed from the perspective of a lifecycle which demonstrates Figure 5 – Business process management lifecycle.

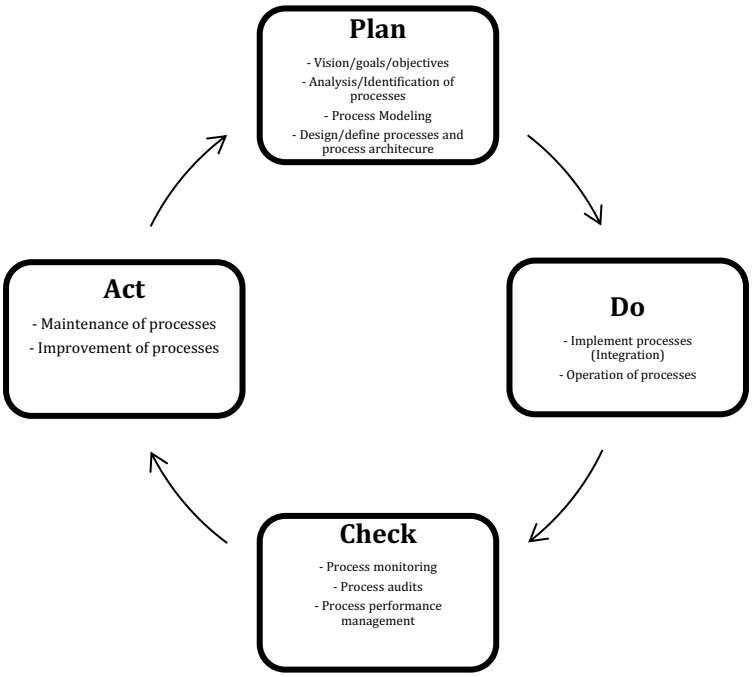

Figure 5 – Business process management lifecycle

2.4 Methods for the identification and assessment of existing processes

Most organizations already have processes in place. On the basis of (Information Systems Audit and Control Association, n.d.), for process management it is necessary to:

1) identify those processes,
2) analyze the processes and their maturity,
3) define the necessary processes and the needed maturity,
4) fill the gap between the actual processes and the needed processes/process maturity.

A basic method to identify actual processes – which the author of this thesis developed – is the following top down approach:

1) Business analysis – deriving high level respectively generic processes by analyzing the business of the organization. A good starting point is the organization chart and

interviews with departments like organization, quality management or controlling. A first differentiation of the processes in core, management and support processes is done.

2) Specification of processes – is done by conducting interviews to
   a) identify input, output and functions/activities
   b) identify chronological and logical sequence
   c) identify objectives of the process
   d) identify process owner, process manager and process actors

   Result is a detailed structure of processes (normally five to eight processes per department). Every process is autonomous. Processes normally contain three to ten functions and are logically completed.
3) Structuring of processes – sometimes the same or similar process is identified in different departments with other names. Such redundancies are now identified and consolidated. Processes are now arranged in a process map using their input/output or logical/chronological relations. Processes are now interlinked with other processes.

For the practical identification of existing processes also newer methods to identify processes like (Leopold, Pittke, & Mendling, 2013) are available. In this thesis, the identification of ISMS core processes is done by analyzing relevant standards (chapter 3) and using specific criteria (chapter 5.1) instead of conducting interviews because a generic framework will be developed and there is no single organization which is analyzed regarding their existing processes. Nevertheless the method described is practically relevant for every user of the developed framework.

For the assessment of processes several methods already exist like:

- ISO/IEC 15504 Process Assessment (International Organization for Standardization and International Electrotechnical Commission, 2003, 2004a, 2004b, 2008, 2012a, 2013)– consists of three process categories, nine groups, 48 processes and six capability levels (Hwang, 2009). The assessment of the capability of the processes is done using attribute ratings in ISO 15504-2 (International Organization for Standardization and International Electrotechnical Commission, 2003):
  - Process performance
  - Performance management
  - Work product performance
  - Process definition
  - Process deployment
  - Process measurement
  - Process control
  - Process innovation
  - Process optimization

- ISO/IEC 33000 series – The ISO 33000 series contain actually five standards, which are replacing the ISO 15504 series:
  - ISO/IEC 33001 "Information technology – Process assessment – Concepts and terminology" – contains definitions and concepts involved for process assessment, capability, conformance and conformity assessment
  - ISO/IEC 33002 "Information technology – Process assessment – Requirements for performing process assessment" – contains the concept of assessment itself
  - ISO/IEC 33003 "Information technology – Process assessment – Requirements for process measurement frameworks" – contains the requirements regarding a process measurement framework for each process quality attribute.
  - ISO/IEC 33004 "Information technology — Process assessment — Requirements for process reference, process assessment and maturity models" – contains process reference models, process assessment models and maturity models.
  - ISO/IEC 33020 "Information technology — Process assessment — Process measurement framework for assessment of process capability" – contains the requirements for measuring process capability in accordance with ISO/IEC 33003
- COBIT Process Assessment Model (Information Systems Audit and Control Association, n.d.-d) – adapts the COBIT content into an ISO 15504 compliant process assessment model and contains

  - Process reference model – describing COBIT processes with process description, purpose, outcomes and work products (output) including a definition which output is input to which other process or supports other processes and base practices (functions/activities)
  - Measurement framework – using a capability model and process attribute ratings similar to ISO 15504-2 (International Organization for Standardization and International Electrotechnical Commission, 2003)
  - Assessment process – containing the following steps
    - Initiation
    - Planning
    - Briefing
    - Data collection
    - Data validation
    - Process attribute rating
    - Assessment reporting

    and the process attribute ratings of ISO 15504-2 (International Organization for Standardization and International Electrotechnical Commission, 2003).

- ISO/IEC 38500 (*Information technology -- Process assessment -- Process measurement framework for assessment of process capability*, 2015b) – is a standard for corporate

governance of information technology consisting of a framework of principles to use when evaluating, directing and monitoring the use of IT:

- Responsibility
- Strategy
- Acquisition
- Performance
- Conformance
- Human Behavior

The framework also consists of definitions and a model. Also main definitions of governance and management are clearly defined. The standard is also intended to inform and guide in designing and implementing the management system of policies, processes, and structures that support governance.

Maturity models will be discussed later in chapter 4 State of the art – capability and maturity level models.

An adequate method for the determination of the necessary maturity level will be developed or identified later by analyzing the capability and maturity level models (described in chapter 7 Method to determine the necessary maturity level) in depth.

3 State of the art – security management

In this chapter, an overview of relevant and actual security management standards is given. The established standard will be briefly described in the following.

In relevant standards and frameworks as well as in the literature the continuous increasing dependency of nearly all organizations on appropriate secure information processing was stated practically in the last years (German Federal Office for Information Security, 2008, p. 5; Martins & Elofe, 2002; Sambamurthy et al., 2003). Standards for the management of information security and collections of best practice measures were developed and established (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013), (German Federal Office for Information Security, 2008), (German Federal Office for Information Security, 2013). Beside national standards like NIST SP 800 series in the US (U.S. Department of Commerce - National Institute of Standards and Technology, n.d.) or the IT security guidelines from the Federal Office for Information security in Germany (German Federal Office for Information Security, 2013) the most important standards for the development and operation of an information security management system (hereinafter referred to as "ISMS") are the ISO 270xx, ITIL and COBIT (Stoll, 2014). The same standards were identified as most used standards for IT governance and IT management followed by CMM and CMMI, PRINCE2 and PMBOK in an ISACA study (Information Systems Audit and Control Association, 2008, p. 26).

Also a lot of references are recognizing ISO 270xx as the most widely accepted information security standard next to initiatives as COBIT and ITIL: (Baldassarre, 2016; Dombora, 2016; Nicho & Muamaar, 2016; Schwickert & others, 2017; Sowa, 2017a; Susanto et al., 2011), et cetera. Some authors are also recognizing ISO 38500 as a relevant standard. This standard is not used in this thesis because ISO 38500 contains a process assessment model and no information about ISMS processes itself.

3.1 ISO 27000 series

The International Organization for Standardization (hereinafter referred as "ISO") and the International Electrotechnical Commission (hereinafter referred as "IEC) formed a joint technical committee – ISO/IEC JTC 1. The sub-committee SC 27 of this committee has a working group WG 1 which develops and facilitates international standards for information security management systems. ISO 27001 as the international standard from ISO/IEC JTC 1 SC27 WG1 for information security management systems (herein after referred as "ISMS") is the security standard in enterprises (Boehmer, 2008; International Organization for Standardization and International Electrotechnical Commission, 2013).

ISO 27001 contains the requirements for planning, implementing, operating, and improving an information security management system. Requirements are formulated in a general manner to fit for all organizations independent of their size, objectives, business model, location et cetera. In ISO 27001 absolutely no requirements are formulated for any specific technology (Brenner, 2007) but the standard contains requirements for ISMS core process. Therefore, this standard forms the basis to identify ISMS core processes.

The ISO 27000 series does not only contains ISO 27001. Another common standard for information security of the ISO 27000 series is ISO 27002 (International Organization for Standardization and International Electrotechnical Commission, 2013) containing controls that should be implemented with the ISMS. ISO 27002 is linked with ISO 27001 with an Annex of ISO 27001 listing the controls of ISO 27002. Further ISO 27000 series standards are:

- ISO 27000 – ISMS – Overview and vocabulary
- ISO 27003 – Information security management system implementation guidance
- ISO 27004 – Information security management — Measurement
- ISO 27005 – Information security risk management
- ISO 27006 – Requirements for bodies providing audit and certification of ISMS
- ISO 27007 – Guidelines for ISMS auditing
- ISO 27008 – Guidance for auditors on ISMS controls
- ISO 27010 and following – sector specific standards
- ISO 27030 and following – standards for technical controls and guidelines for controls of ISO 27002

3.2 ITIL

The IT Infrastructure Library (ITIL), specified in (Office of Government Commerce, 2007a, 2007b, 2007c, 2007d, 2007e, 2007f), is a best practice framework for IT service management. IT service management is the management of all processes that co-operate to ensure the quality of live IT services, according to the levels of service agreed with the customers(Publishing, 2007). The primary objective of service management is to ensure that IT services are aligned to the business needs and actively support them (Office of Government Commerce, 2007a). ITIL was developed by the Central Computing and Telecommunications Agency – today Office of Government Commerce – and is today available in the third version.

ITIL contains five books:

- Service strategy (Office of Government Commerce, 2007e) – is a guideline for designing and implementing service management as strategic asset. Service strategy ensures the management of costs and risks of the service portfolio. While not only focusing on operational efficiency, it also ensures holistic and sustainable services.

- Service Design (Office of Government Commerce, 2007a) – provides instructions for the development and design of services and processes. Design principles and methods are presented to transform strategic goals in a portfolio of services and service assets.
- Service Transition (Office of Government Commerce, 2007f) – contains information about the development and improvement of capabilities regarding the implementation of new or changed services into production.
- Service Operation (Office of Government Commerce, 2007d) – is focusing on the operation of IT services regarding efficiency and effectiveness.
- Continual Service Improvement (Office of Government Commerce, 2007b) – contains instructions for the recurring improvement of design, implementation and operation of IT services (continual improvement process)

ISO/IEC 20000 (International Organization for Standardization and International Electrotechnical Commission, 2011a, 2012b) is the international standard for service management containing the requirements of a service management system while ITIL provides a body of knowledge for achieving those requirements (Office of Government Commerce, 2007a).

In this thesis, the generic process reference model of ITIL and ISO/IEC 20000 are used as an orientation to define the ISMS core process model and to identify interfaces of ISMS core processes to IT service management processes.

3.3 COBIT

Control Objectives for Information and related Technology (COBIT), specified in (Information Systems Audit and Control Association, n.d.-a), (Information Systems Audit and Control Association, n.d.-b), (Information Systems Audit and Control Association, n.d.-d) is a control framework to help an organization ensure alignment between use of information technology and its business goals (Ridley, Young, & Carroll, 2004). COBIT is based on five key principles (Information Systems Audit and Control Association, n.d.-a):

1) Meeting stakeholder needs
2) Covering enterprise end-to-end
3) Applying a single, integrated framework
4) Enabling holistic approach
5) Separating governance from management

COBIT also contains a process reference model, generic process capability attributes and a process assessment model which describes how to execute a capability assessment in an efficient and effective way. A key concept in COBIT is the determination and systematic enhancement of process maturity (Information Systems Audit and Control Association, 2008, p. 18).

COBIT will be analyzed with the aim to use or adapt the process reference model for the use with ISMS core processes. Capability levels in COBIT are (Information Systems Audit and Control Association, n.d.-d):

1) Incomplete process
2) Performed process
3) Managed process
4) Established process
5) Predictable process
6) Optimized process

Furthermore a COBIT 5 Professional Guide for Information Security (Information Systems Audit and Control Association, n.d.-c) is provided which focusses on information security and provides more detailed and more practical guidance

Mappings and integrations between/of COBIT, ITIL and ISO/IEC27000 series are available (Sahibudin, Sharifi, & Ayat, 2008; Von Solms, 2005). In this thesis the COBIT family is used to identify ISMS core processes and to integrate maturity levels in the ISMS core process framework.

3.4 Conclusions

As the aforementioned standards are identified as the most important standards for the development and operation of an information security management system in the following the ISO 270xx, ITIL and COBIT will be used to identify ISMS core processes.

Core principle of those standards is the Plan-Do-Check-Act cycle as identified in (International Organization for Standardization and International Electrotechnical Commission, 2013) and (German Federal Office for Information Security, 2008) which is used to structure ISMS processes.

All mentioned standards are alive and actually used as the following exemplarily references will justify:

- ISO 27000 series:
  - (Sowa, 2017b)
  - (Alexander & Panguluri, 2017)
  - (Santos, Rebelo, & Silva, 2017)
- ITIL:
  - (Cots, Casadesús, & Marimon, 2016)
  - (Krabbes, 2016)
  - (Barafort, Mesquida, & Mas, 2016)
- COBIT:
  - (Scholderer, 2016)
  - (Drljača & Latinović, 2017)
  - (Laita & Belaissaoui, 2017)

4 State of the art – capability and maturity level models

In this chapter an overview of relevant and actual capability and maturity level models is given to choose or later develop (see chapter 6 Maturity Level Model for ISMS core processes) an appropriate maturity level model for ISMS core processes. According to von Wangenheim, Hauck, Salviano, and von Wangenheim (2010) as a result of a systematic literature review on capability/maturity models most models are concentrated around the CMM/CMMI framework and the standard ISO/IEC 15504 (SPICE). ISO/IEC 15504 has a broad international acceptance and dominance (Meroth et al., 2015; Salviano & Figueiredo, 2008) as well as it has itself a high level of maturity. As the ISO/IEC 33000 series is intended to replace the ISO/IEC 15504 standard this is also a standard suite which need to be analyzed. Miloslavskaya and Sagirov (2016) and Stevanović (2011a) identified O-ISM^3 and SSE-CMM as another two most important capability maturity models. Also the Program Review for Information Security Management Assistance (PRISMA) (Bowen & Kissel, 2007a) methodology from the U.S. National Institute of Standards and Technology (NIST) was taken into consideration as a relevant standard. PRISMA includes five maturity levels: policies, procedures, implementation, testing and integration. PRISMA focusses on the whole ISMS or a whole information security program and is therefore not process oriented. Because of that PRISMA is not analyzed further in this thesis.

Primary the following frameworks and standards will be analyzed:

- CMMI (CMMI Product Team, 2010a, 2010b, 2010c),
- ISO/IEC 15504, also known as SPICE (International Organization for Standardization and International Electrotechnical Commission, 2004a),
- ISO/IEC 33000 series (mainly ISO/IEC 33004 (*Information technology -- Process assessment -- Requirements for process reference, process assessment and maturity models*, 2015) and ISO/IEC 33020 (*Information technology -- Process assessment -- Process measurement framework for assessment of process capability*, 2015a))
- O-ISM^3 (Canal, n.d.) and
- ISO/IEC 21827, also known as SSE-CMM (*Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)*, 2008).

Maturity models can be described as set of elements that describe certain aspects of improvement (maturity) in the organization (Stevanović, 2011b). The idea behind a Capability Maturity Model (CMM) is that an organization with more mature processes has a higher capability level than a less mature organization, while “more mature” is defined as “processes are better defined and managed” (Phillips, 2003a). The presence of mature ISMS-processes does not guarantee any success of the ISMS but it provides some insight into the ability of the ISMS to maintain an adequate information security level (Phillips, 2003a). In the following state of the art of standards regarding capability and maturity level models will be described.

4.1 CMMI

The idea of CMMI(CMMI Product Team, 2010a, 2010b, 2010c) goes back to Richard Nolan's "staged model (Nolan, 1973), which was applied by the Software Engineering Institute of Carnegie Mellon University as Software Capability Maturity Model (SW-CMM) later followed by the CMM Integrated (herein after referred as "CMMI") (Publishing, 2007). CMMI is known as the standard in maturity modelling.

CMMI provides a model for continuous improvement of processes as well as a staged model (Publishing, 2007). In the continuous model improvement is measured using capability levels for a particular process. In the staged model improvement is measured using maturity levels for a set of processes.

Capability Levels in the continuous model are (CMMI Product Team, 2010c):

1) Incomplete process – is a process that either is not performed or is partially performed one or more of the specific goals of the process area are not satisfied and no generic goals exist for this level.
2) Performed process – is a process that accomplishes the needed work to produce work products. The specific goals of the process area are satisfied.
3) Managed process – is a performed process that is planned and executed in accordance with policy; employs skilled people having adequate resources to produce controlled outputs; involves relevant stakeholders; is monitored, controlled and reviewed; and is evaluated for adherence to its process description.
4) Defined process – is tailored from the organization's set of standard processes according to the organization's tailoring guidelines, and contributes work products, measures and other process improvement information to organizational process assets.
5) Quantitatively managed process – is a defined process that is controlled using statistical and other quantitative techniques.
6) Optimizing process – is a quantitatively managed process that is improved based on an understanding of the common causes of variation inherent in the process.

Maturity levels in the stages model are (CMMI Product Team, 2010c):

1) Initial – processes are a hoc and chaotic
2) Managed – processes are planned and executed in order with policy. Responsibility and resources are assigned as well as people are trained to perform the processes. Relevant stakeholders are identified and involved as well as processes are periodically monitored and controlled. Process adherence is periodically evaluated and process performance is shared with senior management.

3) Defined – processes are well characterized and understood, and are described in standards, procedures, tools and methods. Standards, process descriptions and work procedures are tailored from the organization's set of standard processes according to the organization's tailoring guidelines. A defined process clearly states the purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs and exit criteria.
4) Quantitatively managed – quantitative objectives for quality and process performance are defined and used as criteria in managing processes.
5) Optimizing – processes are continually improved through incremental and innovative process and technological improvements based on a quantitative understanding of the organization's objectives and performance needs.

While this thesis is based on the assumptions that not every ISMS process needs the same degree of maturity level, CMMI will be used to develop a method to identify the necessary maturity level. Prerequisite of this is an analysis and discussion of the applicability for the use of CMMI with an ISMS.

4.2 ISO/IEC 15504

ISO/IEC 15504 – also known as "SPICE – Software Process Improvement and Capability determination" is an international standard for the assessment of processes for software and electronics development and contains a process reference models as well as a process assessment model.

ISO/IEC 15504 consists of the following parts:

- ISO/IEC 15504-1:2004 – Information technology – Process assessment – Part 1: Concepts and vocabulary (International Organization for Standardization and International Electrotechnical Commission, 2004a)
- ISO/IEC 15504-2:2003 – Information technology – Process assessment – Part 2: Performing an assessment (International Organization for Standardization and International Electrotechnical Commission, 2003)
- ISO/IEC 15504-3:2004 – Information technology – Process assessment – Part 3: Guidance on performing an assessment (International Organization for Standardization and International Electrotechnical Commission, 2004b)
- ISO/IEC 15504-4:2004 – Information technology – Process assessment – Part 4: Guidance on use for process improvement and process capability determination (International Organization for Standardization and International Electrotechnical Commission, 2008)
- ISO/IEC 15504-5:2012 – Information technology – Process assessment – Part 5: An exemplar software life cycle process assessment model (International Organization for Standardization and International Electrotechnical Commission, 2012a)

- ISO/IEC 15504-6:2013 – Information technology – Process assessment – Part 6: An exemplar system life cycle process assessment model (International Organization for Standardization and International Electrotechnical Commission, 2013)

Inspired in the continuous model of CMMI (individual maturity level for every process), in ISO 15504 the continuous model of CMMI is used. The capability levels are identical with CMMI continuous representation.

Assessment of process attributes is done by using the levels

N — Not achieved
P — Partially achieved
L — Largely achieved
F — Fully achieved

The COBIT 5 process assessment model is also based on the process assessment model of ISO/IEC 15504 (Information Systems Audit and Control Association, n.d.-d, p. 7).

4.3 ISO/IEC 33000 series

The ISO/IEC 33000 series contain actually five standards, which are replacing the ISO 15504 series. In this series the standard ISO/IEC 33004:2015 “Information technology — Process assessment — Requirements for process reference, process assessment and maturity models” – contains requirements regarding process reference models, process assessment models and maturity models.

According to ISO/IEC 33004 a process reference model is a defined set of processes that collectively can support the primary aims of a community of interest. A process reference model provides the basis for one or more process assessment models where a process assessment model is related to one or more process reference models. A process assessment model forms the basis for the collection of evidence and rating of a process quality characteristic.

According to ISO/IEC 33004 “A maturity model is derived from one or more specified process assessment model(s) that identifies the process sets associated with each of the levels in a scale of organizational process maturity, and relates to the growing ability of an organization to achieve higher levels of a specific process quality characteristic.”

A declaration of scope for a maturity model is necessary and may take the form of a description of the domain of application and the specific aspects of that domain that are addressed.

Process capability levels are defined in ISO/IEC 33020 (*Information technology -- Process assessment -- Process measurement framework for assessment of process capability*, 2015a) as follows:

- Process capability level 0: Incomplete process
  - The process is not implemented, or fails to achieve its purpose.
  - There is little or no evidence of any systematic achievement of the process purpose.
- Process capability level 1: Performed process
  - The process achieves its process purpose.
- Process capability level 2: Managed process
  - The performed process is implemented in a managed fashion (planned, monitored and adjusted)
  - The work products of the process are appropriately established, controlled and maintained.
- Process capability level 3: Established process
  - The managed process is implemented using a defined process that is capable of achieving its process outcomes.
- Process capability level 4: Predictable process
  - The established process operates predictively within defined limits to achieve its process outcomes.
  - Quantitative management needs are identified, measurement data are collected and analyzed to identify assignable causes of variation.
  - Corrective action is taken to address assignable causes of variation.
- Process capability level 5: Innovating process
  - The Predictable process is continually improved to respond to change aligned with organizational objectives.

The organizational maturity levels are also described in ISO/IEC 33020 (*Information technology -- Process assessment -- Process measurement framework for assessment of process cabability*, 2015a) as follows:

- Maturity level 0 (immature)
- Maturity level 1 (basic)
- Maturity level 2 (managed)
- Maturity level 3 (established)
- Maturity level 4 (predictable)
- Maturity level 5 (innovating)

4.4 O-ISM³

The Open Group announced an information security management standard – The Open Group Information Security Management Maturity Model (The Open Group, 2011) (herein after referred as "O-ISM³"), which enables the creation of ISMS that are fully aligned with any organization's business mission and compliance needs regardless of size, context and resources ("The Open Group | The Open Group Releases Maturity Model for Information Security Management," n.d.). The Open Group is a vendor-neutral and technology-neutral consortium ("The Open Group | The Open Group Releases Maturity Model for Information Security Management," n.d.).

Core concepts of O-ISM³ are designing the system using maturity levels and using a process-oriented approach toward ISM (Canal, 2008). O-ISM³ is built from the best ideas of management systems and controls from ISO 9000, ITIL, CMMI and ISO27001 (Canal, 2008). The major difference between ISO 27001 and O-ISM³ is that the second has maturity levels, while ISO 27001 takes a compliant/non-compliant approach built around controls (Narayanan, 2010). O-ISM³ can be used as a tool to implement a business oriented ISMS and further the ISMS can be certified as per ISO 27001(Narayanan, 2010).

ISM process model as defined in the O-ISM³ contains processes at the following levels:

- General Processes like document management, ISM system and business audit and design and evolution
- Strategic management processes like report to stakeholders, coordination, strategic vision
- Tactical management processes like security awareness, disciplinary process, background checks
- Operational management processes like security procurement, inventory management or software development lifecycle control

Each process is described by a description, value the process produces, documentation regarding the process, inputs and outputs, metric descriptions, responsibilities, related processes and related methodologies. Also a guide to apply security performance metrics and maturity levels to an established ISO 27001 ISMS is available (The Open Group, 2014).

In this thesis beside ISO 27000 series O-ISM³ is used as a basis to identify ISMS core processes, while O-ISM³ not only contains processes where the process owner is the ISMS. So the ISM process model of O-IMS³ needs to be reduced to ISMS core processes.

4.5 ISO/IEC 21827 – SSE-CMM

System Security Engineering Capability Maturity Model (SSE-CMM) – also known as ISO/IEC 21827 – describes the basic characteristics that an organization must provide in order to achieve the admissible level of information security (Stevanović, 2011b).

ISO/IEC 21827:2008 does not prescribe a particular process or sequence (International Organization for Standardization and International Electrotechnical Commission, 2009).

SSE-CMM is intended to be used as a basis for designing ISMS and provides a model for assessing the security maturity level exist (International Organization for Standardization and International Electrotechnical Commission, 2009):

- Level 1 – Base practices are performed informally
- Level 2 – Base practices are planned and tracked
- Level 3 – Base practices are well defined
- Level 4 – Base practices are quantitatively controlled
- Level 5 – Base practices are continuously improving

The SSE-CMM defines the following security related process areas (International Organization for Standardization and International Electrotechnical Commission, 2009):

- Process area 01 – Administer Security Controls
- Process area 02 – Assess Impact
- Process area 03 – Assess Security Risk
- Process area 04 – Assess Threat
- Process area 05 – Assess Vulnerability
- Process area 06 – Build Assurance Argument
- Process area 07 – Coordinate Security
- Process area 08 – Monitor Security Posture
- Process area 09 – Provide Security Input
- Process area 10 – Specify Security Needs
- Process area 11 – Verify and Validate Security

For every process area that is important from the security aspect, SSE-CMM identifies entities that are being followed and that are measurable (Stevanović, 2011b). Security attributes that follow it and that represent the basis for measurements are added to every entity (Stevanović, 2011b).

While ISM3 is oriented on business result achievement, which is on the top of the priority list, SSE-CMM is focused primarily on information security, and the effect on business is measured during the implementation (Stevanović, 2011b).

In this thesis beside ISO 27000 series SSE-CMM is used as a basis to identify ISMS core processes with the process areas of SSE-CMM and as a basis for the capability maturity model.

4.6 SAMM – Strategic alignment maturity assessment

Strategic Alignment Maturity Model (SAMM) was developed by Jerry Luftman and is focused on business-IT alignment, but can also be adapted to business-information security alignment. Luftman (2000) also uses five levels of strategic alignment maturity:

1. initial/ad hoc processes
2. committed processes
3. established focused processes
4. improved/managed process
5. optimized processes

Each level focuses on a set of six criteria:

1. communications maturity
2. competency/value measurement maturity
3. governance maturity
4. partnership maturity
5. scope and architecture maturity
6. skills maturity

In SAMM also a strategic alignment process is defined consisting of:

1. set the goals and establish a team
2. understand the business-IT-linkage
3. analyze and prioritize gaps
4. specify the actions (project management)
5. choose and evaluate success criteria
6. sustain alignment

The ideas and concepts of Luftman (2000) are used in this thesis as an inspiration and a basis for choosing or later develop (see chapter 6 Maturity Level Model for ISMS core processes) an appropriate maturity level model for ISMS core processes as well as the development of a method to determine the necessary maturity level of ISMS core processes (see chapter 7 Method to determine the necessary maturity level).

4.7 Conclusions

According to several studies e.g. (Lasrado, Vatrapu, & Andersen, 2015; Poeppelbuss, Niehaves, Simons, & Becker, 2011) in information systems research, maturity models are widely used. Furthermore they are well understood and developed over decades.

Maturity models can be used as benchmark comparison tool. The level of improvement depends on processes and their specific objectives to support general objectives of an organization (Stevanović, 2011b).

The described state of the art of standards regarding capability and maturity level models form a good basis for choosing or later develop (see chapter 6 Maturity Level Model for ISMS core processes) an appropriate maturity level model for ISMS core processes.

All mentioned models are alive and actually used as the following exemplarily references will justify:

- CMMI
  - (Chaudhary & Chopra, 2017)
  - (Yeh et al., 2017)
- ISO/IEC 15504
  - (Kasulke & Bensch, 2017)
  - (Uskarcı & Demirörs, 2017)
- ISO/IEC 33000 series
  - (Mehairjan, 2017)
  - (Kirinic & Kozina, 2016)
- O-ISM^3
  - (Suwito, Matsumoto, Kawamoto, Gollmann, & Sakurai, 2016)
  - (Ormrod & Turnbull, 2016)
- ISO/IEC 21827
  - (Alpar et al., 2016)
  - (Mohamed, Baharom, Deraman, Yahya, & Mohd, 2016)
- SAMM
  - (Ernerot & Torstensson, 2017)
  - (Spósito, Neto, & da Silva Barreto, 2016)

Part III – Contribution

5 ISMS core process framework

As the first key element of the contribution part, this chapter contains an analysis of the latest research as well as an analysis of the most relevant security management standards regarding mentioned ISMS processes to answer the main research question MRQ1-2 “Are there defined ISMS processes existing in established standards?” and MRQ1-3 “Are there defined ISMS processes existing in the latest ISMS process framework research?”.

The first part of this chapter contains the identification, evaluation and discussion of criteria for identifying processes as ISMS core processes.

The second part of this chapter contains the results of a systematic literature review (SLR) regarding the latest ISMS process framework research.

In the third part of this chapter the in chapter 3 described standards will be analyzed regarding the ISMS processes they contain to answer the main research question MRQ1-2 “Are there defined ISMS processes existing in established standards?”. Chapter 5.4.2 contains a matrix of analyzed standards and contained ISMS processes.

In the fourth part of this chapter the ISMS core process criteria are applied to the possible ISMS core processes to discuss if the process is an ISMS core process, management process, supporting process or other process.

The result of this discussion is an ISMS core process framework which is described and illustrated in a process framework in the fifth part of this chapter and will answer MRQ1-4 ”What is the agreed basis of ISMS processes in existing standards and in the latest ISMS process research work?”

5.1 Development of criteria for identifying processes and ISMS core processes

Later in this chapter, the frameworks and standards – identified as state of the art – will be analyzed and compared regarding the description of ISMS core processes. As a prerequisite of that, criteria for the categorization as ISMS core process will be developed and verified within a study. By using the developed criteria to identify ISMS core processes, the applicability of those criteria will be tested and additionally verified indirectly by conducting an expert study regarding the identified ISMS core processes (see chapter 5.2).

As defined in chapter 2.2, core processes deliver apparent and direct customer value and are derived from the core competencies of an organization. As a result of this from the perspective of the ISMS a core process

1) is derived from or related to the core competencies of the ISMS and
2) delivers apparent and direct value to the stakeholder

What is a core competency?

Javidan (1998) defines competencies as a set of skills and know-how housed in a strategic business unit. Competencies also require resources and capabilities. (Javidan, 1998) defines a core competency as a collection of competencies that are widespread in the corporation and they result from the interaction between different strategic business units competencies.

By applying this definition to the ISMS, the core competency of the ISMS is a collection of competencies of the ISMS. According to (Calder & Watkins, 2010) the core competency of the ISMS is the assessment of information security risks. Beside this risk treatment is another necessary core competency of the ISMS to effectively and efficiently manage the risks of information security. Only considering this two core competencies would be a too narrow point of view to identify core processes. To achieve a core competency several competencies are necessary. Therefore in the further analysis ISMS core processes are derived from the competencies of the ISMS instead from the two mentioned core competencies.

As already mentioned, competencies are a set of skills and know-how housed within the ISMS. To answer the question if a process is a competency of the ISMS we need to ask – based on (Javidan, 1998) – four questions:

- Are the necessary know how and skills present in the ISMS to perform the process very well?
- Is the process managed or even owned by the ISMS / the information security officer? This means that the information security officer is accountable for the whole process and as the process owner he defines objectives of the process derived from the objectives of the ISMS which will be defined by the top management. The information security officer is responsible for the process design (Information Systems Audit and Control Association, n.d.-d, p. 128). In many practical cases – especially in small organizations – the information security officer will also be the process manager who is responsible for the process operation.
- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS?
- Does the competency support the two identified core competencies risk assessment and risk treatment?

What is an apparent and direct value and what are the stakeholders of the ISMS?

Value reflects the owners/buyers desire to retain or obtain a product (Neap & Celik, 1999). The owners of the ISMS or buyers of the products of the ISMS are the stakeholder of the ISMS, which is in the first the organization, which implements the ISMS respectively the top management of this organization. The product of the ISMS is continuously achieving the information security objectives, set by the top management, while complying with any constraints also set by the top management.

Given that, the amount of value generated by a specific process will differ as the information security objectives are different for every organization. As a result the specific amount of value generation cannot be measured at this generic level of the analysis.

To solve this problem, a process is supposed to deliver direct value to stakeholders if the output of the process is intended to achieve or maintain the achievement of an information security objective.

What in general is a process?

A process is a set of interrelated or interacting activities which transforms inputs into outputs (International Organization for Standardization and International Electrotechnical Commission, 2005).

Thinking about processes in general means asking what need to be done at a regular basis, how are those tasks interrelated and interacting and which inputs are transformed into which outputs – resulting in input-transformation-output processes (Slack, Chambers, & Johnston, 2010).

So in general processes are differentiated from one-time tasks or a set of one-time-tasks grouped to a project. Applying this to the PDCA cycle of the ISMS, processes are mainly operated – but not limited to – as part of the DO and CHECK phases of the PDCA cycle). Tasks, which are done once while planning and developing or improving the ISMS in the PLAN and ACT phases of the PDCA cycle can also contain parts which need to be repeated at a regular basis and therefore integrated in operational processes, but are mainly organized as one-time projects. Recognizing that processes can also be of strategic or tactical nature, core processes are mainly operational processes of a management system, which need to be repeated at a regular basis. Strategic or tactic processes are primarily management processes. As this general criteria can only be evaluated in the context of the ISMS it will be considered as specific ISMS process criteria.

What criteria are derived from the aforementioned considerations?

As a result of the aforementioned considerations the criteria for identifying ISMS core processes need to be differentiated into general process criteria and specific ISMS process criteria.

General process criteria two answer the question if something is a process are:

- General process criteria 1 – Regularity – interrelated and interacting tasks are repeated on a regular basis
- General process criteria 2 – Transformation – inputs are transformed into outputs

Specific ISMS process criteria to answer the question if a process is an ISMS core process are:

- ISMS core process criteria 1 – Operational – process is carried out while operating the ISMS
- ISMS core process criteria 2 – Core competency – the process is a core competency of the ISMS and the information security officer is the process owner or process manager
- ISMS core process criteria 3 – Value generating – delivers apparent and direct value to the stakeholder

5.2 Verification of the developed process criteria

5.2.1 Method

To verify if the identified criteria are the most relevant and correct criteria for ISMS core processes the author of this thesis conducted a study. In this study 90 participants were asked to name criteria to identify ISMS core processes in form of a questionnaire. Given was a differentiation in core, management and support processes. None of the criteria identified by the author of this thesis was given in the study to avoid any bias of the participants.

5.2.2 Sample

A panel of 90 German experts in the field of information security was selected, from which 75 experts answered the questionnaire. Roles of the experts were: 53 Information security officers/managers (23 working for private companies; 30 working for public administration), 8 consultants for information security (8 working for private companies), 14 auditors for information security (3 working for public administration; 11 working for private companies)

5.2.3 Results and discussion of the results

From the answers of the participants named criteria where clustered with regards to the content and counted.

The results of this study are documented in Table 1 – Results of the study to identify criteria for ISMS core processes and Appendix C – Results of the ISMS core criteria study

Named criteria by participants of the study	How often was the criteria cited?
Repeatability / Regularity	60 (80%)
Transformation of input into output	41 (55%)
Defined responsibilities and accountabilities	34 (45%)
Information security officer or manager is the process owner	61 (81%)
Defined start and end of the process	29 (39%)
Value generation	60 (80%)
Essential for reaching the objectives of the organization	22 (29%)
Process is operated in the ISMS	62 (83%)

Table 1 – Results of the study to identify criteria for ISMS core processes

The mostly named criteria (80% or more of the participants of the study named that criteria) are:

- Repeatability / regularity (confirming general criteria 1 – regularity)
- Information security officer or manager is the process owner (confirming partially the ISMS core process criteria 2 – core competency)
- Value generation (confirming ISMS core process criteria 3 – value generation)
- Process is operated in the ISMS (confirming ISMS core process criteria 1 – operational)

The criteria "Transformation of input into output was named only by 55% of the participants of the study. One possible explanation for this could be that this is a very basic criteria for processes and not an exclusive criteria for ISMS core processes. So it is supposed that most participants simply forgot naming that criteria. So it is concluded that the general process criteria 2 "Transformation" is also confirmed as a criteria.

Another two criteria "Defined responsibilities and accountabilities" and "Defined start and end of the process "were named by 45% and 39% of the participants of the study. Because those are mainly criteria to identify a maturity level of a process and not to identify a process itself, those criteria is not used in this thesis.

Interesting is that 29% of the participants named a criteria "Essential for reaching the objectives of the organization". This shows that the participants recognized the importance of aligning information security with business objectives. But to conclude, that an ISMS core process must be essential for reaching objectives of the organization would be going too far. So this criteria is also not directly used in this thesis. Instead it is counted as an indicator for ISMS specific criteria of "value generation", as value generation is linked with the objectives of the organization.

In summary the results of the study confirmed the formerly identified criteria for ISMS core processes.

5.3 SLR – Analysis of the latest ISMS process framework research

To answer MRQ1-3 "Are there defined ISMS processes existing in the latest ISMS process framework research?" a systematic literature review (SLR) has been conducted. A systematic review is "a means of evaluating and interpreting all available research relevant to a particular research question, topic area or phenomenon of interest" (Keele, 2007). "Systematic literature reviews in all disciplines allow us to stand on the shoulders of giants and in computing, allow us to get off each other's feet" (Keele, 2007). On the basis of (Kitchenham, 2004, p. 2) the reasons for performing this SLR were:

1. To identify if there is a gap in the current research regarding ISMS process frameworks
2. To provide background in order to appropriately position new research activities (to develop such a framework)

The SLR was performed using the following steps based on (Kitchenham, 2004):

1. Planning the review:
   a) Identification of the need for a review
   b) Development of a review protocol
2. Conducting the review
   a) Identification of research
   b) Selection of primary studies
   c) Study quality assessment
   d) Data extraction and monitoring
   e) Data analysis
3. Reporting the review

5.3.1 Planning the review

5.3.1.1 The need for a systematic review

According to Kitchenham (2004) "The need for a systematic review arises from the requirement of researchers to summarize all existing information about some phenomenon in a thorough and unbiased manner." In this case all defined or proposed ISMS processes in the available ISMS research need to be identified to answer MRQ-1 "Of which elements does the agreed ISMS core process framework consists?" as objective of the SLR.

To identify if any existing SLR regarding ISMS processes are available the following databases were searched with the search strings "SLR" AND "ISMS":

- IEEE – 4 results, none of them containing an SLR about ISMS processes
- ACM – 126 results, the top 13 most relevant results does not contain any SLR about ISMS processes, the following results were excluded simple by reading the title.

- Science direct – 252 results, the top 26 most relevant results does not contain any SLR about ISMS processes, the following results were excluded simply by reading the title like "Evidence for extinct 135Cs from Ba isotopes in Allende CAIs"

As a result, no primary study was found regarding ISMS processes, which arises the need to perform an own SLR. The following restrictions regarding the search for primary studies are present:

- Research string could be to narrow: This limitation will be dealt with in the performed SLR. A broader search string must be constructed to avoid overlooking any relevant research.
- The searched databases could not be the most relevant databases: According to (Kitchenham, Budgen, & Brereton, 2011; Turner, 2010) the searched databases are the most relevant databases. Additionally a search with google scholar and the same search strings was conducted which does not result in the identification of any further relevant research."

5.3.1.2 Review protocol

The review protocol is included as Appendix F – Review protocol for the SLR regarding ISMS process framework.

5.3.1.3 The research question

According to Kitchenham (2004) "the critical issue in any systematic review is to ask the right question. In this context, the right question is usually one that:

- Is meaningful and important to practitioners as well as researchers.
- Will lead either to changes in current "…" practice or to increased confidence in the value of current practice.
- Identify discrepancies between commonly held beliefs and reality.

Additionally Kitchenham (2004) states that "a systematic review in a PhD thesis should identify the existing basis for the research student's work and make it clear where the proposed research fits into the current body of knowledge."

The research question MRQ1-3: "Are there defined ISMS processes existing in the latest ISMS process framework research?" will identify the existing basis to answer MRQ1: "Of which elements does the agreed ISMS core process framework consists?". This will result in reaching objective 1 – Develop an ISMS core process framework. An ISMS core process framework will fit into the existing current body of knowledge as agreed ISMS standards like ISO 27001 stipulate the planning and implementation of ISMS processes but does not provide a clear process framework of the ISMS.

5.3.2 Conducting the review

5.3.2.1 Generating a search strategy

The following strategy was used for the construction of search terms:

A. Use the research question for the derivation of major terms
B. For these major terms, find the alternative spellings and synonyms;
C. Use of Boolean operators for conjunction in such a way, to use 'OR' operator for the concatenation of alternative spellings and synonyms whereas 'AND' for the concatenation of major terms.

The research question MRQ 1 consists of two groups of terms:

- Group 1: Information security terms
  - ISMS
  - Information Security Management System
  - Information Security
- Group 2: Process framework terms
  - Process framework
  - Process reference model
  - Process model
  - Process
  - Processes

The resulting search string is the following:

"ISMS" OR "Information Security Management System" OR "Information Security" AND "Process framework" OR "Process reference model" OR "Process model" OR "Process" OR "Processes"

5.3.2.2 Study selection criteria

Regarding the selection of the search strategy respectively the search tools and databases the following factors were taken into account:

For performing the search it is essential, that the search tools or databases offer features for an easy evaluation of the search results like for example showing how often an item has been cited. For efficiency reasons it is important to get fast access and have the possibility to export bibliographic data to Zotero which is used by the author of this thesis as a reference management tool.

Based on Kitchenham et al. (2011) and Turner (2010) the following most relevant databases were searched:

- IEEE
- ACM
- Science direct

To avoid publication bias the search string was also used to scan for relevant literature using google scholar.

The following table contains the search process documentation in detail

#	Name of the database or other source	search string	Date of the search	years covered by the search (see EC1)	number of results
1	IEEE	*(ISMS OR Information Security Management System OR Information Security) AND (Process Framework OR Process reference model OR Process model OR Process OR Processes)* *search in full text and metadata using advanced search*	April 5rd 2016	January 2015 till April 2016	881 (after applying EC1: 132)
2	ACM	*("ISMS"; "Information Security Management System"; "Information Security Management"; "Information Security") AND ("process reference model"; "process model"; "process"; "processes")* *search in the ACM Full Text Collection using advanced search*	April 5rd 2016	January 2015 till April 2016	337 (after applying EC1: 55

#	Name of the database or other source	search string	Date of the search	years covered by the search (see EC1)	number of results
3	Science direct	*"ISMS" OR "Information Security Management System" OR "Information Security Management" OR "Information Security" AND "Process framework" OR "Process reference model" OR "Process model" OR "Process" OR "Processes" AND LIMIT-TO(topics, "system,security,model,risk")* search in all fields using expert search of science direct	April 5rd 2016	January 2015 till April 2016	5206 (after applying EC1: 426)
4	Google Scholar	*"ISMS" OR "Information Security Management System" OR "Information Security Management" OR "Information Security" AND "Process framework" OR "Process reference model" OR "Process model" OR "Process" OR "Processes"*	April 5rd 2016	January 2015 till April 2016	ca. 486.000 (after applying EC1: 22.900)
5	Google Scholar	*("ISMS" OR "Information Security Management System" OR "Information Security Management" OR "Information Security") AND ("Process framework" OR "Process reference model" OR "Process model")*	April 5rd 2016	January 2015 till April 2016	9750 (after applying EC1: 750)

Table 2 – Search process documentation – SLR ISMS processes

5.3.2.3 Performing the study selection process

The following selection criteria of the results were defined by the author of this thesis:

- Exclusion criteria – EC1: Exclude any study or paper which is older than January 2015

- Exclusion criteria – EC2: Exclude any study/paper where the title suggests that the paper is not focused on ISMS or ISMS processes and the title is not available in English or German.
- Exclusion criteria – EC3: Exclude any study/paper where the abstract shows the paper is not focused on ISMS and process frameworks.
- Inclusion criteria – IC1: Include all studies or papers which does not meet one of the exclusion criteria EC1 to EC3

The first search with Google Scholar produced 486.000 hits. Even by applying EC1 22.900 hits were left. Screening the results showed that a majority of the identified papers/studies would be excluded by using EC2. It is supposed that the reason for that is the too broaden search string. So the keywords "Process" and "Processes" were removed as they are too general. The resulting refined search string is:

("ISMS" OR "Information Security Management System" OR "Information Security Management" OR "Information Security") AND ("Process framework" OR "Process reference model" OR "Process model")

The second search with Google Scholar with the refined search string produced 9.750 hits. After applying EC1 750 hits were left which were analyzed regarding the exclusion criteria EC2. Searching with the refined search string in IEE, ACM and Science direct does not produce any reduction in the search results.

Within the screening of the titles all papers or studies were excluded if the title suggests that a different topic than ISMS or ISMS processes is the focus of the paper. For example the following papers were obviously not focused on the research question and therefore excluded:

- Design of Integrated Analytical Process Framework for Smart City Transformation based on Strengths-Weaknesses-Opportunities-Threats Analysis.
- A comprehensive and harmonized digital forensic investigation process model
- Application of Fuzzy Analytical Hierarchy Process in the Safety Evaluation of Computer Network
- Calculation Model of the Status and Staffing for Security Management-A Case Study
- A new Software Testing Process Model-Track Model

After applying EC2 to the results of the Google Scholar search 175 studies and papers were left. After applying EC2 to the results of the Science direct search 56 studies and papers were left. After applying EC2 to the results of the ACM search 18 studies and papers were left. After applying EC2 to the results of the IEEE search 34 studies and papers were left.

After applying the exclusion criteria EC1 and EC2 the remaining results were assessed regarding the exclusion criteria EC3. For the assessment of the inclusion criteria IC1 it is considered critical to assess the abstract of the papers/studies regarding the question does the abstract shows the paper is focused on ISMS and process frameworks?

After the exclusion of irrelevant papers based on title and abstract and the exclusion of doublets, the researcher finally found the following papers or studies which meet the inclusion criteria IC1 and should be included in the data extraction and analysis:

- Towards a document-driven approach for designing reference models: From a conceptual process model to its application (Frank, 2016)
- Information security management needs more holistic approach: A literature review (Soomro, Shah, & Ahmed, 2016)
- A Framework for Information Security Governance and Management (Carcary, Renaud, McLaughlin, & O'Brien, 2016)

The selection process and the results of that process are shown in Figure 6 – Analysis of the latest ISMS process framework research.

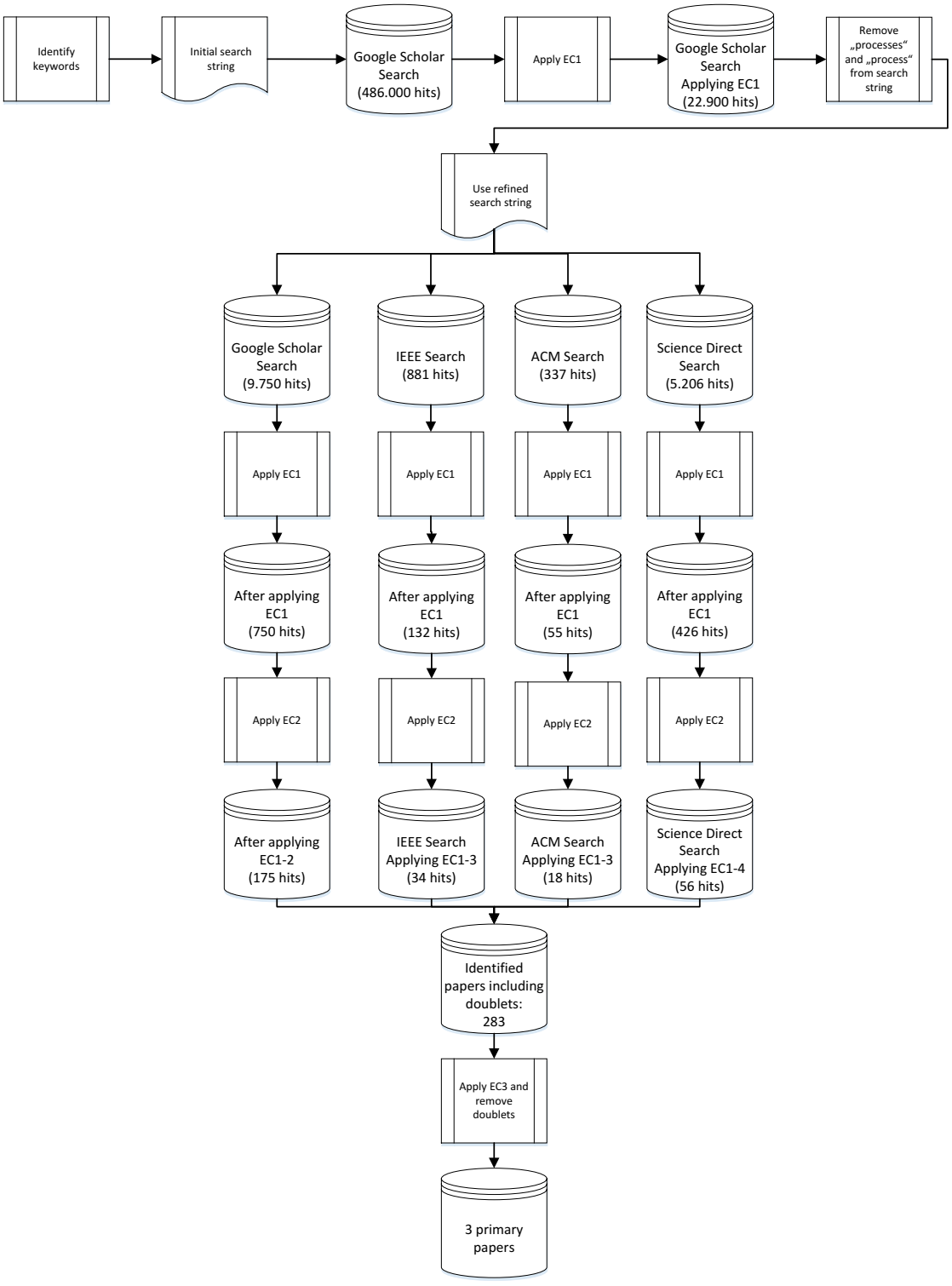

Figure 6 – Analysis of the latest ISMS process framework research

5.3.2.4 Study quality assessment

According to Kitchenham (2004) in addition, to general inclusion exclusion criteria, it is generally considered important to assess the "quality" of primary studies but there is no agreed definition of study "quality".

As described in Carcary et al. (2016) the results of this study rely on:

- the comparison of standards
- several academic and practitioner literature analysis and
- insights from subject matter experts.

As described in Soomro et al. (2016) the results of this study rely on a systematic literature review. As described in Frank (2016) a scientific approach consisting of four steps was used. First, a requirements framework for designing reference models was developed. Second, the framework was used as a basis for the comparison of well-documented reference models. Thereafter, the gained insights from step one and two were consolidated into a conceptual process model that has a strong regard to preexisting knowledge. Finally, a case study has showed the applicability of the determined model.

Considering this information the quality hierarchy of the identified papers is evaluated as follows (most important is quality hierarchy 1):

#	Paper	SLR	Expert opinion	Case study	Quality hierarchy
1	Towards a document-driven approach for designing reference models: From a conceptual process model to its application (Frank, 2016)	-	-	X	3
2	Information security management needs more holistic approach: A literature review (Soomro et al., 2016)	X	-	-	2
3	A Framework for Information Security Governance and Management (Carcary et al., 2016)	X	X		1

Table 3 – Study quality assessment – SLR ISMS processes

5.3.2.5 Data extraction and analysis, limitations and conclusion

In order to answer MRQ1-3 "Are there defined ISMS processes existing in the latest ISMS process framework research?" three primary papers have been identified. Most of the candidates can be described as noise because

- they were not focusing on information security management,
- were focusing on general process management or specific topics actually in the focus of interest like cyber security or cloud security, or
- were not directly related to a ISMS process framework.

Independent of what is presented in the resulting three papers, because of the low number of identified papers an agreed basis of ISMS processes in the latest ISMS process research work cannot be derived. Nevertheless the main ideas of the identified papers are discussed below.

The resulting three papers are:

- A Framework for Information Security Governance and Management (Carcary et al., 2016)
- Information security management needs more holistic approach: A literature review (Soomro et al., 2016)
- Towards a document-driven approach for designing reference models: From a conceptual process model to its application (Frank, 2016)

In Carcary et al. (2016) it is recognized that initially, information security management was regarded as a technical activity, but now it is shifting to an approach that reflect the importance of embedding information security within organizational structures. This is only possible within an integrated management system consisting of ISMS processes with interfaces to other domains of a management system. In Carcary et al. (2016) a framework of information security governance and management activities is proposed. This framework claims to be activity-oriented but does not name any ISMS processes directly. The named activity categories are:

- Governance
- Technical security
- Security resource management
- Security risk control
- Security data administration
- Business continuity management

Those categories contain some activities which could lead to ISMS processes. Other categories like technical security or security data administration seems not to lie in the accountability of the ISMS. This will be analyzed further in chapter 5.3 on the basis of the established security management standards.

In (Soomro et al., 2016) a literature analysis was done to synthesize management's roles in information security to explore specific managerial activities to enhance information security management. They found that numerous activities of management, particularly development and execution of information security policy, awareness, compliance training, development of effective enterprise information architecture, IT infrastructure management, business and IT alignment and human resources management, had a significant impact on the quality of management of information security. While this managerial activities lead to ISMS processes, which will also be analyzed further in this chapter 5.3 on the basis of the established security management standards, some of the named literature in this paper will also be used in this thesis.

In Frank (2016) it is recognized that reference models have demonstrated to be a beneficial instrument for providing blue prints for a reasonable, good design of information systems and underlying organizational settings. This is an important insight as in this thesis a reference model for ISMS core processes will be developed to solve the problem of the missing reference model of ISMS core processes (see chapter 1.2 Significance of the thesis), which could be used as such a blueprint. They found, that benefits like time savings, cost savings, and quality increases are only realized, if the reference model is research-based, empirically evaluated and profoundly documented. These criteria are also adopted as objectives of this thesis. Further in this paper a conceptual process model for designing reference models is presented. It is also concluded that information security research tends to design models encapsulated from each other by often neglecting already existing research. This will be avoided in this thesis by analyzing the latest research of ISMS process frameworks (see chapter 5.1) as well as the use of maturity level models within an ISMS (see chapter 6).

While the first two papers recognize ISMS activities they fail to compose a holistic process model from those activities and they do not differentiate enough between activities in the responsibility of the ISMS and activities which lie in the responsibility of other management system domains – like IT infrastructure management and technical security. So both papers are a good starting point to develop ISMS processes, but they do not represent any ISMS process research itself. The last paper is more of general interest while developing reference models, but again it does not contain any research regarding ISMS process frameworks itself.

Limitations

EC 1 could be a too narrow criteria for this systematic literature review because resigning EC 1 would significantly increase the list of papers and studies. But it was the objective of this SLR to identify only the latest research on ISMS process frameworks. Even a quick search with Google Scholar without any time limitation only one relevant additional paper (Mangin, Barafort, Heymans, & Dubois, 2012) was found dealing with ISMS process frameworks, which was formerly excluded because it is from 2012. So EC1 seems to be appropriate.

Also the chosen search engines could be a too narrow criteria for this systematic literature review but for instance using a Google search with the string “Information security process framework” produced no further relevant papers.

Conclusion

The fact that only three papers were found meeting the inclusion criteria after applying the exclusion criteria validates that there is a lack of attention in the latest research for ISMS process frameworks.

Taking into account the content of the identified three papers, which does not contain any ISMS process framework research in a narrower sense, it must be concluded that there is

no agreed basis of ISMS processes in the latest ISMS process research work – because ISMS process research work is not present at an reliable level.

As a result of this the proposed ISMS process framework will be derived mainly from existing standards rather from latest research papers or studies.

5.4 Analysis of security management standards

In this part of this chapter the in chapter 3 described standards will be analyzed regarding the ISMS processes they contain to answer the main research question MRQ1-2 "Are there defined ISMS processes existing in established standards?". Chapter 5.4.2 contains a matrix of analyzed standards and contained ISMS processes.

In the following

- the ISO 27001 standard statements on processes will be *analyzed*
- *for the purpose* of comparing it
- *with respect to* the degree of coverage and relationship with specific processes in ITIL and COBIT favoring reuse
- *from the viewpoint of* process management and management in general
- *in the context of* organizations interested in planning, implementing and operating a process based information security management systems

This analysis intends to support and guide any organization in harmonizing, integrating, managing, and aligning its information security management processes in other management system processes by using the ISO 27001, ITIL and COBIT models. In this sense, the contribution is twofold and can be formalized in two research questions supporting MRQ1-2 that set out the research goal stated above in detail:

- MRQ1-2-a: Which are the defined ISMS processes existing in established standards?
- MRQ1-2-b: To what extent are the practices described in the ISO 27001, ITIL and COBIT models related?

To answer those research questions, multiple process reference models (ISO 27001, ITIL and COBIT) need to be harmonized.

Baldassarre, Caivano, Pino, Piattini and Visaggio (2012) presented a strategy that guides the harmonization of multiple process reference models through a systematic stepwise approach, general enough to be applied to any reference models that are being taken into account. The harmonization strategy of Baldassarre is based on the process and the framework for supporting multi-model harmonization of (Pardo, Pino, García, Piattini, & Baldassarre, 2010).

According to Baldassarre et al. (2012) "In general, the harmonization framework defines as follows: (1) A guideline for determining the harmonization goals, based on the strategic plan and goals defined in the organization's mission; (2) A harmonization process for driving multi-model harmonization, with which to manage and lead the harmonization of models step by step; (3) A harmonization ontology, which presents the terms, concepts and relationships for supporting the harmonization models, and (4) A Set of Techniques and Methods, which facilitates the configuration and definition of the harmonization strategies. The harmonization strategy is the work product resulting from the implementation of the harmonization process.

As the harmonization process a theoretical comparison process is used, because mapping is one of the most widely used strategies for the harmonization of models (Baldassarre et al., 2012). The purpose of this process is to perform a step-by-step comparison and a mapping of different models, aiming to guarantee the reliability of obtained results. For the theoretical comparison the ISO 27001 standard was considered as a starting model, as this is the most important standard for information security management (Stoll, 2014).

The outcome of the theoretical comparison process is a table (Result of Comparison) that maps the models and points out the relationships between them (based on (Calvo-Manzano, Cueva, & Muñoz, 2008)) regarding the mentioned ISMS processes.

For the analysis of the identified security management standards a modified (steps 5 and 6) similarity method based on the Models and Standards Similarity Study method of (Calvo-Manzano et al., 2008) was used.

The original method contains the following steps:

1. **Select the models and standards to be analyzed** – this step is documented in chapter 3
2. **Choose the reference model** – as reference model the ISO 27000 series is chosen because resulting from the focus of this standard series the widest coverage of ISMS processes is expected.
3. **Select the process** – The selection of the processes and the selected processes are described in chapter 5.4.1
4. **Establish a detail level** – as all analyzed standards are international standards and are applicable to all organizations independent of their size, objectives, business model, location et cetera – the contained information about ISMS processes are generic. Therefore a similar detail level is chosen to analyze the standards.
5. **Create a correspondence template** – Instead of a detailed correspondence template a process profile template was created. This is included in Appendix A – Process Profiles.
6. **Identify the similarity among models** – The process templates were completed with information obtained from the standards. This is included in Appendix A – Process Profiles.
7. **Show obtained results** – The obtained results are described in chapter 5.4.2

5.4.1 Identification of processes

For this thesis the terms matching and mapping are differentiated as follows:

Matching is the process of identifying two semantically related processes (Predoiu et al., 2005). Processes are semantically related if they are represented in two or more standards with the same or different terms. The interpretation rules to decide if there are semantically related processes are characterized as implicit rules for mapping knowledge about a base domain (ISO 27000 series) into a target domain (Gentner, 1983). Beside this, a comparison scale has been defined and used. The scale contains the following elements based on the scale presented by Baldassarre et al. (2012):

A. **Strongly related (S):** the process is especially named in the standards and the process has the same process objectives and contain the same process steps
B. **Partially related (P):** the process is not especially named, but there are one or more requirements in the standard which lead to the implementation of the process defined in another standard
C. **Weakly related (W):** the process is not especially named, but there is a process or a process concept which can/should be adapted in an ISMS.
D. **Non-related (N)**: no relationship can be identified.

In the step of matching, the comparison is performed through an iterative and incremental procedure. The process used, that was adapted from (Baldassarre et al., 2012), is iterative, because the comparison (analysis and determination of the relationship between the ISO 27001 and ITIL/COBIT) is executed completely on one ISMS process first, and then on the others in turn. It is also incremental, in the sense that the comparison outcome (i.e., the final product of the theoretical comparison process) grows and evolves with each iteration until it becomes the final one. Using this, iterative and incremental approach was necessary to deal with the complexity entailed in a comparison in which entities of low-level abstraction are involved.

For the identification of processes the following method was used:

1. Initially the ISO 27000 series were analyzed regarding mentioned processes. For that an atomization of the requirements of ISO 27001 was done and the atomized requirements were analyzed regarding mentioned processes. The result of this is documented in Appendix E – Results of atomization of ISO 27001. The general process criteria regularity and transformation were then used to verify if the mentioned processes are generally processes. The result of this task is documented in chapter •

2. ITIL and COBIT were analyzed (matching) regarding ISMS processes which were already identified in the ISO 27000 series as well as regarding additional possible ISMS processes. In the context of the matching the following questions were asked (based on (Calvo-Manzano et al., 2008)):
   a) Is there any information about ISMS processes in the other standards related to ISMS processes of the reference standard (ISO 27000 series)? What is the additional information that could help to carry out the ISMS process of the reference standard?
   b) Is there any information about possible additional ISMS processes in the other standards? What is this information / what is the possible additional ISMS process?

   A matching table regarding the possible ISMS processes was created for ITIL and COBIT. The result of this task is documented in chapter 0 and chapter 5.4.1.3

3. The results from steps one and two were summarized in a mapping table which is documented in chapter 5.4.2

Mapping refers to the combination of the standards/processes. After the identification of semantically related processes they are combined into an integrated process framework by using a mapping (Gentner, 1983). Matching and mapping are established methods in scientific knowledge comparison (Guo & Kraines, 2008) and especially used to compare and merge different ontologies (Gentner, 1983; Predoiu et al., 2005):

- (Anam, Kim, Kang, & Liu, 2016)
- (Ramar & Gurunathan, 2016)
- (Donnelly, 2017)
- (Haufe, Colomo-Palacios, Dzombeta, Brandis, & Stantchev, 2016)
- (Sanchez-Gordón, Colomo-Palacios, & Herranz, 2016)
- (Larrucea, Santamaría, & Colomo-Palacios, 2016)

5.4.1.1 ISO 27000 series

This section describes ISMS processes derived initially from (International Organization for Standardization and International Electrotechnical Commission, 2010a, 2013, 2013). The initial and most high-level process regarding ISMS is described in ISO 27003 as an **ISMS planning process** (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 2):

- Obtaining management approval for initiating an ISMS
- Defining ISMS Scope and ISMS Policy
- Conducting Organization Analysis
- Conducting Risk Assessment and Risk Treatment planning
- Designing the ISMS

As this is the reference standard the requirements of ISO 27001 were atomized and clustered to possible ISMS-processes. The detailed results of this work are contained in Appendix E – Results of atomization of ISO 27001. As a result of this analysis and according to ISO 27001 ISMS process candidates, which need to be designed, are:

- **information security risk assessment process** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 3) which is an overall process of risk analysis and risk evaluation (International Organization for Standardization and International Electrotechnical Commission, 2014, p. 5)
- **information security risk treatment process** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 4) which is a process to select and implement measures to modify risk (International Organization for Standardization and International Electrotechnical Commission, 2014, p. 5). Controls are now determined during the process of risk treatment, rather than being selected from Annex A of ISO 27001 (BSI UK, 2013, p. 4)
- **resource management process**, which ensures that necessary resources are determined and provided (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 5)
- **processes to assure necessary awareness and competence** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 5), where the process of creating awareness may be regarded as part of communication (BSI UK, 2013, p. 12)
- **communication processes** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 6), including internal and external communication as well as marketing for the ISMS
- **documentation and records control process** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 6,7)
- **requirements management process** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 1,7)
- **information security change management process** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 7)
- **process to control outsourced services** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 7)
- **performance evaluation process** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 7,8) containing **monitoring** (the performance of ISMS need to be monitored in terms of verification and reporting of security control implementation), **measurement** (a measurement system to evaluate performance in information security management and feedback suggestions for improvement need to be established (International Organization for Standardization and International Electrotechnical Commission, 2014, p. 11)), analysis and evaluation
- **internal audit process** in terms of planning and conducting internal audits as part of an audit program (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 8)

- **management review process (information security governance process)** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 8)
- **information security improvement process** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 9)
- **information security incident management process** (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 7, 2014, p. 11)

The following table contains the discussion of the general process criteria to answer the question if the identified process candidates are really processes:

#	process candidate	general process criteria 1 – regularity	general process criteria 2 – transformation	decision
1	ISMS planning process	Some of the outputs of this process – like management approval, scope definition – need to be checked regular regarding their actuality and appropriateness, but the process itself is primary an initial process which is carried out once as a project (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 5). The regular activities like renewing the management approval are also integrated in the management review and improvement processes.	In the ISMS planning process inputs like the vision of the stakeholders are transformed into outputs like the management approval for the ISMS or the ISMS scope.	It is not a process because it lacks the required regularity.

#	process candidate	general process criteria 1 – regularity	general process criteria 2 – transformation	decision
2	Information security risk assessment process	The information security risk assessment process is the overall process of risk analysis and risk evaluation. The information security risk assessment process should be monitored, reviewed and repeated regularly (International Organization for Standardization and International Electrotechnical Commission, 2011, pp. 22–23). Several iterations of this process are often conducted (International Organization for Standardization and International Electrotechnical Commission, 2011, pp. 9–10).	Input from ISMS planning process, information assets and previous process results are transformed into documented and evaluated risks and risk owners.	It is a process.
3	Information security risk treatment process	The information security risk treatment process is the overall process to identify and select risk treatment options as well as control objectives and controls. As this process is a part of the risk management process it should be monitored, reviewed and repeated regularly (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 4).	In the information security risk treatment process documented and evaluated risks are transformed into a risk treatment plan.	It is a process.
4	Resource management process	The resource management process needs to be carried out at a regular basis because it is integrated in the ISMS an continuously supports the ISMS processes as well as the controls by identifying, allocation and monitoring of required resources. So this is not a one-time task.	The resource management process transforms input like initial ideas of controls and the design of ISMS processes into planned, documented and monitored resources to run the ISMS processes and to implement potential controls	It is a process.

#	process candidate	general process criteria 1 – regularity	general process criteria 2 – transformation	decision
5	Process to assure necessary awareness and competence	This process need to be carried out regularly because requirements, risks and controls as well as the employees/personnel are continuously changing.	This process transforms input like awareness requirements, policies and security objectives into awareness plans, materials and finally an adequate awareness level of all employees.	It is a process.
6	Communication process	Risk communication is the process to achieve agreement on how to manage risks by exchanging and/or sharing all information about risks between the decision-maker and other stakeholders. Risk communication should be performed continually	(International Organization for Standardization and International Electrotechnical Commission, 2011, p. 22). In the risk communication process input like information about risks and information needs of stakeholders are transformed into risk communication plans. Information needs of the stakeholders are satisfied.	It is a process.
7	Documentation and records control process	Documentation and records control process is the process to identify, create, update and control information determined to be necessary for the effectiveness of the ISMS. As updating and maintaining the relevant documentation is part of the process it must be carried out regularly.	In the documentation and records control process output of other ISMS processes are transformed into appropriate and managed documentation.	It is a process.
8	Requirements management process	As it is necessary to continually keep the identified requirements up-to-date this process is performed regularly.	The process transforms input like stakeholder expectations and other constraints into documented and assigned requirements.	It is a process.

#	process candidate	general process criteria 1 – regularity	general process criteria 2 – transformation	decision
9	Information security change management process	Information security change management is the process to control changes of ISMS elements and review the consequences of unintended changes. This process only focusses on change management of the ISMS. As the operational environment of the organization changes regular, ISMS elements like security measures also need to be changed regularly.	Input like proposed changes and needs for changes are transformed into implemented and documented changes.	It is a process.
10	Process to control outsourced processes	Taking into account changes of requirements, service providers and of the operational environment the process to control outsourced services needs to be repeated on a regular basis like the management of information security within the organization.	Within the process to control outsourced services inputs like requirements are transformed into specific phrases in contracts or request for changes.	It is a process.
11	Performance evaluation process	The performance of an ISMS should be monitored regularly (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 63). The performance of controls like continuity controls should also verified regularly (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 73). Both, the performance evaluation of ISMS processes as well as the performance evaluation of controls is realized with the performance evaluation process.	Input like control lists and control objectives are transformed into monitoring/measurement activities as well as records of those activities and finally in management reports.	It is a process.

#	process candidate	general process criteria 1 – regularity	general process criteria 2 – transformation	decision
12	Internal audit process	As the results of this process are input for the regularly evaluation of the ISMS this process must performed regularly too (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 41,55).	Input like control lists, control objectives and incident reports are transformed into audit plans, audit reports and finally in management reports.	It is a process.
13	Information security improvement process	Continuous improvement of the ISMS and the information security controls are stipulated by ISO 27001 (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 9) Improvement contains not only regular reviews of the ISMS with the management to align the ISMS with the governing stakeholder needs and expectations which is realized with the information security governance process. Improvement also contains regular improvements of efficiency, effectiveness, suitability and adequateness of the ISMS processes and of the information security controls which is realized with the information security improvement process. Taking into account that the improvement process requires a continuous scanning and monitoring of the internal and external environment, emerging technology and innovations as well as a regular processing of improvement suggestions the process must be repeated on a regular basis.	Input like suggestions for improvement and nonconformities are transformed into request for changes to realize the improvement or to eliminate root causes of non-conformities.	It is a process.

#	process candidate	general process criteria 1 – regularity	general process criteria 2 – transformation	decision
14	Information security governance process	The management should initiate management reviews to continually improve the suitability, adequateness and effectiveness of the ISMS (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 9). Output of the management review contains decisions related to governing the ISMS. Taking into account the objective to governing the ISMS the information security governance process must be repeated on a regular basis.	Input like management reports are transformed into decisions related to the governance of the ISMS and related change requests.	It is a process.
15	Information security incident management process	Information security incidents should be detected and responded to in a timely manner (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 63). While it is not clear when and how often information security incidents occur, information about potential information security incidents are gathered regularly (Howard & Longstaff, 1998) and a continual proactive identification of information security incidents is conducted (Humphreys, 2008).	Potential information security incidents and gathered information related to them are transformed into incident report, changes and are the basis for updating risk evaluations and training/awareness controls.	It is a process.

Table 4 – Process identification from ISO 27001

As shown in Table 4 – Process identification from ISO 27001 except "ISMS planning process" all ISMS process candidates have been identified as processes.

5.4.1.2 ITIL

This section describes service management processes derived initially from (Office of Government Commerce, 2007a, 2007b, 2007c, 2007d, 2007e, 2007f), (International Organization for Standardization and International Electrotechnical Commission, 2011, 2012b).

Service management processes, which need to be designed, are:

- General processes
  - **documentation control process** (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 9)
  - **resource management process** (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 10)
  - **internal audit process** (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 12)
  - **management review process** (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 12)
  - **improvement process** (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 13)
- Service delivery processes
  - **service level management process** (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 15)
  - **performance evaluation process** (International Organization for Standardization and International Electrotechnical Commission, 2012b, p. 16)
  - **service reporting process**
  - **service continuity and availability management process**
  - **Budgeting and accounting for services process**
  - **Capacity management process**
  - Information security management process
    - **Information security risk assessment process**
    - **Information security change management process**
    - **Process to control outsourced processes**
    - **Internal audit process**
    - **Information security incident management process**
- Relationship processes
  - **Business relationship management process**
  - **Supplier management process**
- Resolution processes
  - **Incident and service request management process**
  - **Problem management process**
- Control processes
  - **Configuration management process**
  - **Change management process**
  - **Release and deployment management process**

A matching between all relevant ITIL processes and the already identified processes from ISO 27001 was conducted. Table 5 – Matching of identified ISMS processes to ITIL processes contains the result of this matching.

ISMS processes of ISO 27000 series	ITIL process	Relation
ISMS planning process	No equivalent in ITIL	Non-related
Information security risk assessment process	As part of the information security management process (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 18)	Strongly related
Information security risk treatment process	No equivalent in ITIL	Non-related
Resource management process	Comparable to the budgeting and accounting for services process and also see (Brenner, 2007, p. 10)	Partially related
Process to assure necessary awareness and competence	No equivalent in ITIL	Non-related
Communication process	No equivalent in ITIL	Non-related
Documentation control process	Documentation control process	Strongly related
Requirements management process	Beside service level management process no direct equivalent in ITIL	Weakly related
Information security change management process	As part of the information security management process (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 19)	Strongly related
Process to control outsourced processes	As part of the information security management process (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 19) and supplier management process	Strongly related
Performance evaluation process	Performance evaluation process	Strongly related
Internal audit process	As part of the information security management process (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 18) and also see (Brenner, 2007, p. 12)	Strongly related
Information security improvement process	Improvement process	Partially related
Information security governance process	Included in the management review process	Partially related
Information security incident management process	As part of the information security management process and the incident and service request management process (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 19)	Strongly related

Table 5 – Matching of identified ISMS processes to ITIL processes

Table 6 – Possible ISMS processes of ITIL not mentioned in ISO 27001 series contains possible ISMS processes of ITIL which are not mentioned in the ISO 27001.

Possible ISMS processes of ITIL not mentioned in the ISO 27000 series	Relation	comment
Service level management process	Non-related	No equivalent in ISO 27001
Service reporting process	Non-related	No equivalent in ISO 27001
Service continuity and availability management process	Weakly related	As part of the risk treatment measures are chosen in the information security risk treatment process
Budgeting and accounting for services process	Partially related	Comparable to the resource management process
Capacity management process	Weakly related	As part of the risk treatment measures are chosen in the information security risk treatment process
Business relationship management process	Non related	No equivalent in ISO 27001
Information security customer relationship management process (as part of the business relationship management process)	Non related	No equivalent in ISO 27001
Supplier management process	Partially related	As part of process to control outsourced processes
Incident and service request management process	Partially related	Incident management is a separate process in the ISMS. The accountability of an integrated incident and service request management process could be assigned to the ISMS or SMS manager.
Problem management process	Non related	No equivalent in ISO 27001
Configuration management process	Non related	No equivalent in ISO 27001
Change management process	Non related	No equivalent in ISO 27001
Release and deployment management process	Non related	No equivalent in ISO 27001

Table 6 – Possible ISMS processes of ITIL not mentioned in ISO 27001 series

As ITIL is a process oriented framework the verification if the identified processes are really processes with the use of the general process criteria is obsolete but is done nevertheless to ensure consistency of the approach. The following table contains the discussion of the general process criteria to answer the question if the identified process candidates (see Table 6 – Possible ISMS processes of ITIL not mentioned in ISO 27001 series) are really processes.

#	process candidate	general process criteria 1 – regularity	general process criteria 2 – transformation	decision
1	**Service level management process**	**The service level management process need to be performed at a regular basis, because the catalogue of services shall be maintained following changes to services and SLAs to ensure that they are aligned** (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 16)**.**	**Input like customer requirements, potential costs and technical constraints are transformed into agreed services.**	**It is a process.**
2	**Service reporting process**	**Service reports are regularly produced for services using information from the delivery of services and the SMS activities to enable decisions of the service provider and take actions based on the findings in service reports** (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 16)**. So this process is performed at regular frequency and at in the operational phase of the service management system.**	**It transforms input like performance and other measures and trend information into a service report**	**It is a process.**
3	**Service continuity and availability management process**	**Maintaining a service continuity plan and an availability plan requires a regular performance of this process.**	**The process transforms input like customer requirements regarding availability in availability and continuity plans.**	**It is a process.**

#	process candidate	general process criteria 1 – regularity	general process criteria 2 – transformation	decision
4	**Budgeting and accounting for services process**	**Like the change management process the budgeting and accounting for services process need to be performed when changes are planned and at a regular frequency because regular monitoring and reporting of costs is also part of this process** (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 17)**.**	**In the budgeting and accounting for services process direct and indirect costs for services are identified to enable an effective financial control and approval. In the process costs of individual components as well as indirect costs are transformed into overall costs of an service** (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 17)**.**	**It is a process.**
5	**Capacity management process**	**Maintaining a capacity plan requires regular measurement and regular performance of this process.**	**The process transforms input like customer requirements regarding capacity in a capacity plan.**	**It is a process.**
6	**Business relationship management process**	**It transforms input from the customers – like requirements and complaints – to changes in SLAs or changes regarding the service requirements.**	**The business relationship management process need to be performed at a regular interval because complaints and changes need to be considered in the operation of the services**	**It is a process.**
7	**Supplier management process**	**Supplier management – especially performance monitoring – need to be performed at a regular frequency.**	**The process transforms input like requirements into defined contracts and ensures that contracts are fulfilled by suppliers.**	**It is a process.**

#	process candidate	general process criteria 1 – regularity	general process criteria 2 – transformation	decision
8	**Incident and service request management process**	**Incidents and service requests should be detected and responded to in a timely manner** (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 63). **While it is not clear when and how often incidents occur, information about potential incidents are gathered regularly** (Howard & Longstaff, 1998) **and a continual proactive identification of incidents is conducted** (Humphreys, 2008)**.**	**Potential incidents and gathered information related to them as well as service requests are transformed into incident report, changes and are the basis for updating risk evaluations and training/awareness controls or SLAs.**	**It is a process.**
9	**Problem management process**	**Searching for root-causes should be performed at a regular frequency – where necessary.**	**The process transforms information about incidents into trends, root causes and preventive requests for changes.**	**It is a process.**
10	**Configuration management process**	**Changes to CIs are recorded. This requires a regular execution of the process.**	**The process of the configuration management transforms single information about CIs, changes or problems into a structured, actual and reliable information basis for most ISMS and SMS-processes.**	**It is a process.**
11	**Change management process**	**As the operational environment of the organization changes regular, CIs are changed regularly.**	**Input like proposed changes and needs for changes are transformed into implemented and documented changes. Changes occur at all levels – strategic, tactic and operational.**	**It is a process.**

#	process candidate	general process criteria 1 – regularity	general process criteria 2 – transformation	decision
12	Release and deployment management process	Changes occur at all levels – strategic, tactic and operational. As a nature of operational changes the most changes including emergency changes occur at an operational level. So the deployment management process is also mainly a process which need to be performed at a regular interval.	Input like approved changes are transformed into release and deployment plans which are executed within this process.	It is a process.
13	Information security customer relationship management process (Business relationship management process)	This process need to be performed at a regular interval and at an operational level, because complaints and changes need to be considered in the operation of the ISMS.	The information security customer relationship management process transforms input from the customers – like requirements and complaints – to changes in the ISMS or information security controls.	It is a process.

Table 7 – Process identification from ITIL

As shown in Table 7 – Process identification from ITIL all ISMS process candidates have been identified as processes.

5.4.1.3 COBIT

COBIT includes a process reference model, which consists of 37 governance and management processes (Information Systems Audit and Control Association, n.d.-a, p. 32). The management processes are assigned to one of the four domains align, plan and organize (APO), Build, acquire and implement (BAI), Deliver, service and support (DSS), Monitor, evaluate and assess (MEA). The 37 processes are:

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimization
- EDM04 Ensure Resource Optimization
- EDM05 Ensure Stakeholder Transparency
- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security
- BAI01 Manage Programs and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organizational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration
- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls
- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance with External Requirements

Especially the processes APO013 Manage security, DSS04 Manage continuity and DSS05 Manage security services provide basic guidance on how to define, operate and monitor a system for general security management (Information Systems Audit and Control Association, n.d.-c, p. 13).

To identify all processes in COBIT which could be relevant or part of an ISMS a matching between all COBIT processes and the already identified processes from ISO 27001 and ISO 20000 was conducted.

As COBIT is a process oriented framework the verification if the identified processes are really processes with the use of the general process criteria is obsolete.

Table 8 – Matching of identified ISMS processes to COBIT processes contains the result of this matching.

Process (ISO 27001/20000 process)	COBIT process(es)	Relation
ISMS planning process	EDM03, APO01, APO02, APO03, APO13, BAI08, DSS06	Strongly related
Information security risk assessment process	APO12	Strongly related
Information security risk treatment process	APO05, APO12, APO13, BAI01, BAI03, DSS01	Strongly related
Resource management process	EDM04, APO05	Strongly related
Process to assure necessary awareness and competence	APO07, BAI08	Strongly related
Communication process	BAI08	Partially related
Documentation control process	BAI08	Partially related
Requirements management process	BAI02, APO02, DSS06	Strongly related
Information security change management process	APO13, BAI03	Strongly related
Process to control outsourced processes	DSS01	Strongly related
Performance evaluation process	MEA01, EDM05, APO11, APO13, DSS01	Strongly related
Internal audit process	MEA01, MEA02, MEA03, EDM05, APO11	Strongly related
Information security improvement process	EDM01, EDM03, EDM05, APO01, APO04, APO11, APO13	Strongly related
Information security governance process	EDM01, EDM03, EDM05, APO01, APO04, APO11, APO13	Strongly related
Information security incident management process	DSS05	Strongly related
Service level management process	APO09, DSS06	Strongly related
Service reporting process	MEA01	Strongly related
Service continuity and availability management process	DSS04, BAI04	Strongly related
Budgeting and accounting for services process	APO06	Strongly related
Capacity management process	BAI04	Strongly related

Process (ISO 27001/20000 process)	COBIT process(es)	Relation
Business relationship management process	APO08, EDM02, APO01	Strongly related
Supplier management process	APO10	Strongly related
Incident and service request management process	DSS02	Strongly related
Problem management process	DSS03, APO11	Strongly related
Configuration management process	BAI09, BAI10, BAI08	Strongly related
Change management process	BAI05, BAI06, BAI07, BAI01, BAI03	Strongly related
Release and deployment management process	BAI01, BAI03	Strongly related

Table 8 – Matching of identified ISMS processes to COBIT processes

As shown in Table 8 – Matching of identified ISMS processes to COBIT processes all COBIT processes do have matchings in already identified processes from ISO 27001 and ISO 20000. But the key aspect of EDM02 – ensure benefits delivery – to clearly add and demonstrate a value to the customers with information security investments is not focused in the identified processes. Therefore an additional process "**Information security customer relationship management**" is added to the list of potential ISMS core processes, which is also based on the ITIL process "business relationship management process".

The COBIT process DSS05 refers to security services. In COBIT 5 for information security the following services are mentioned (Information Systems Audit and Control Association, n.d.-c, p. 50):

- Provide a security architecture
- Provide security awareness
- Provide secure development
- Provide security assessments
- Provide adequately secured and configured systems in line with security requirements and security architecture
- Provide user access and access rights in line with business requirements
- Provide adequate protection against malware, external attacks and intrusion attempts
- Provide adequate incident response
- Provide security testing
- Provide monitoring and alert services for security-related events

They provide a service-oriented view on security related activities (Information Systems Audit and Control Association, n.d.-c, p. 50). Those services were either already integrated in or output of the identified ISMS processes like information security controls as output of the information security risk treatment process. Therefore this COBIT process is not additionally considered as separate ISMS process.

5.4.2 Summary of the analysis of security management standards

No standard provides an ISMS process framework including a detailed description of ISMS processes, input, outputs and interfaces of the processes. Table 9 contains a matrix of analyzed standards and the identified possible ISMS processes as identified in chapter 5.4.1 Identification of processes.

The upper part of the table contains processes directly mentioned in the ISO 27001, where the lower part of the table contains possible ISMS processes derived from the other standards. The relation strength of the processes is indicated in parentheses.

Process/standard	ISO 27001	ITIL	COBIT
ISMS planning process	X	– (N)	X (S)
Information security risk assessment process	X	X[1] (S)	X (S)
Information security risk treatment process	X	– (N)	X (S)
Resource management process	X	X[2] (P)	X (S)
Process to assure necessary awareness and competence	X	– (N)	X (S)
Communication process	X	– (N)	X (P)
Documentation and records control process	X	X (S)	X (P)
Requirements management process	X	– (W)	X (S)
Information security change management process	X	X[3] (S)	X (S)
Process to control outsourced processes	X	X[4] (S)	X (S)
Performance evaluation process	X	X (S)	X (S)
Internal audit process	X	X[5] (S)	X (S)
Information security improvement process	X	X (P)	X (S)
Information security governance process	X	X (P)	X (S)
Information security incident management process	X	X[6] (S)	X (S)
Service level management process	–	X (N)	X (S)
Service reporting process	–	X (N)	X (S)
Service continuity and availability management process	(X)[7]	X (W)	X (S)
Budgeting and accounting for services process	(X)[8]	X (P)	X (S)
Capacity management process	(X)[9]	X (W)	X (S)

[1] As part of the information security management process (International Organization for Standardisation and International Electrotechnical Commission, 2011, p. 18)
[2] Comparable to the budgeting and accounting for services process and also see [55, p. 10]
[3] As part of the information security management process (International Organization for Standardisation and International Electrotechnical Commission, 2011, p. 19)
[4] As part of the information security management (International Organization for Standardisation and International Electrotechnical Commission, 2011, p. 19) and supplier management process
[5] As part of the information security management process (International Organization for Standardisation and International Electrotechnical Commission, 2011, p. 18) and also see [55, p. 12]
[6] As part of the information security, incident and service request management process (International Organization for Standardisation and International Electrotechnical Commission, 2011, p. 19)
[7] As part of the risk treatment measures chosen in the information security risk treatment process
[8] Comparable to the resource management process

Process/standard	ISO 27001	ITIL	COBIT
Business relationship management process	–	X (N)	X (S)
Supplier management process	X[10]	X (P)	X (S)
Incident and service request management process	(X)[11]	X (P)	X (S)
Problem management process	–	X (N)	X (S)
Configuration management process	–	X (N)	X (S)
Change management process	–	X (N)	X (S)
Release and deployment management process	–	X (N)	X (S)
Information security customer relationship management process	–	(X) (N)	(X) (W)

Table 9 – Matrix of analyzed standards and contained ISMS processes

5.5 Analysis and classification of ISMS processes

In this part of this chapter the ISMS core process criteria are applied to the possible ISMS core processes to discuss if the process is an ISMS core process, management process, supporting process or other process. For this the results of MRQ1-2 are used to answer MRQ1-4 by applying the criteria to identify the ISMS core processes to the process candidates identified while analyzing the security management standards.

As identified in chapter 5.1 Development of criteria for identifying processes and ISMS core processes the specific ISMS process criteria to answer the question if a process is an ISMS core process are:

- ISMS core process criteria 1 – Operational – process is carried out while operating the ISMS
- ISMS core process criteria 2 – Core competency – the process is a core competency of the ISMS and the information security officer is the process owner or process manager
- ISMS core process criteria 3 – Value generating – delivers apparent and direct value to the stakeholder

5.5.1 ISMS planning process (project)

As identified the ISMS planning process is also not a process, because it is performed mainly once as a project. Nevertheless ISMS core process criteria will be discussed in the following.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – No

The ISMS planning process is performed in the plan phase in the PDCA cycle, which means that the process is not carried out while operating the ISMS (do phase).

[9] As part of the risk treatment measures chosen in the information security risk treatment process
[10] As part of process to control outsourced processes
[11] Incident management is a separate process in the ISMS. The accountability of an integrated incident and service request management process could be assigned to the ISMS or SMS manager.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Partially*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Partially

  Designing/Planning the ISMS is performed before the ISMS is in place. So, even if the necessary know-how is present after implementation of the ISMS, it is not necessarily present before the ISMS implementation. The counting know-how and skills present in the ISMS are focused on operating and optimizing the ISMS. This includes planning skills, which are needed to perform the ISMS processes.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  Formal process owner should be the top management as it is an accountability of the top management to ensure an adequate management of information security. The process manager is regularly the information security officer.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  Regularly competitive know how and skills are nowhere else present in the organization.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  ISMS planning supports the two identified core competencies risk assessment and risk treatment as it defines the necessary fundamentals for that competencies.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – *Yes*

Of course the ISMS designing process is value generating for the top management while it builds the basis for establishing the ISMS, initially provides objectives for the ISMS and initially ensures an ISMS which fulfills the requirements of the top management.

Classification result

Not all criteria of ISMS core processes and not all general process criteria are fulfilled. Therefore it is not categorized as a process and not as an ISMS core process. Nevertheless the ISMS planning process defines the objectives of the ISMS. Because of the importance for the ISMS this "process" is integrated as "ISMS planning project" into the ISMS process framework.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
ISMS planning process	-	X	-	(X)	X	project

Table 10 – Classification of the ISMS planning process/project

5.5.2 Information security risk assessment process

The information security risk assessment process is an overall process of risk analysis and risk evaluation.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

The information security risk assessment process as part of the information risk management process is an integral part of an ISMS and should be applied to the ongoing operation of an ISMS (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 3).

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  General know how and skills regarding risk management as well as the necessary information security know how are present in the information security management system.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  While the process is an integral part of an ISMS the owner of the information security risk assessment process is the information security officer because the information security officer is accountable for achieving the process objective(s) by the top management.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  General know how and skills regarding risk management should be present in the overall risk management system, but the necessary information security know how is only present in the information security management system.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  The process is the core competency of the ISMS.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

The information security risk assessment process is value generating for the top management while it provides documented risks as well as a documented evaluation of those risks which are the basis for proposals for decision.

Classification result

Because all criteria of ISMS core processes are fulfilled the information security risk assessment process is categorized as core process (C).

This process is also part of the service management system (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 18,19). While planning the integration of an information security management system with a service management system this enables synergy effects by planning an integrated instead of two separate processes.

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Information security risk assessment process	X	X	X	X	X	C

Table 11 – Classification of the information security risk assessment process

5.5.3 Information security risk treatment process

The information security risk treatment process (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 4) is the process to select and implement measures to modify risk (International Organization for Standardization and International Electrotechnical Commission, 2014, p. 5). Controls are now determined during the process of risk treatment, rather than being selected from Annex A of ISO 27001 (BSI UK, 2013, p. 4)

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

The information security risk treatment process as part of the information risk management process is an integral part of an ISMS and should be applied to the ongoing operation of an ISMS (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 3).

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  General know how and skills regarding risk management as well as the necessary information security know how are present in the information security management system.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  While the process is an integral part of an ISMS the owner of the information security risk treatment process is the information security officer because the information security officer is made accountable for achieving the process objective(s) by the top management.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  General know how and skills regarding risk management should be present in the overall risk management system, but the necessary information security know how is only present in the information security management system.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  The process is the core competency of the ISMS.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – *Yes*

The information security risk treatment process is value generating for the top management because it provides a documented risk treatment plan, which directly helps the stakeholders to meet their accountability to ensure an appropriate security level.

Classification result

Because all criteria of ISMS core processes are fulfilled the information security risk assessment process is categorized as core process (C).

The information security risk treatment process could also be a management process. Management processes define the objectives of the organization as well as control and monitor the achievement of the objectives at the level of the core processes and the overall organization. They contain project-, quality-, security- and risk management as well as strategic planning. From the viewpoint of the ISMS the information security risk treatment process is not a management process because it defines objectives of controls and no objectives the organization. So it has an operational character.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Information security risk treatment process	X	X	X	X	X	C

Table 12 – Classification of the information security risk treatment process

5.5.4 Resource management process

The resource management process is the process to identify, allocate and monitor required resources to run the ISMS core processes as well as to implement and run the selected controls.

The process details as described in Table 58 – Resource management process were mainly drafted by the author because no specific information about the process is contained in (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2010a).

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

A resource management process is also part of the ISMS planning process. In contrast to the resource management process as part of the ISMS planning this process focusses on the resources necessary to operationally run the ISMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  Taking into account the division of labor the resources necessary to operate the ISMS should be managed by the ISMS itself and necessary know how and skills must be present within the ISMS.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  The accountability of ensuring an adequate and efficient resource usage for information security is clearly assigned to the information security officer.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  In every organization should be an overall resource management process in place. So a competitive know how and skills should also be present outside the ISMS. Taking into account the division of labor the resources necessary to operate the ISMS should be managed by the ISMS itself. Additionally the management of ISMS resources can be operated most efficient and effective within the ISMS as specialized and in depth know how – for example regarding decision making where to spent ISMS resources – are present only within the ISMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  The process provides information like necessary resources to implement and maintain a planned control (part of the core competency "information security risk treatment process") which are necessary in the decision-making process for the risk owners.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

From the viewpoint of the ISMS an efficient resource usage provides a direct value in means of financial terms to the stakeholders of the ISMS.

Classification result

While all other criteria of an ISMS core process are met, the resource management process could nevertheless be a supporting process. Supporting processes provide and manage necessary resources without delivering direct customer value. They support core and management processes. Typical supporting processes are human resources, financial management and IT management. However, from the viewpoint of the ISMS an efficient resource usage provides also a direct value in means of financial terms to the stakeholders of the ISMS. This is achieved by providing information like necessary resources to implement and maintain a planned control, which are necessary in the decision-making process for the risk owners. Therefore, the risk owners are the direct customers of this process. Considering this the results of this process provide a direct customer value.

While integrated in the context of an overall resource management process the operational resource management process of ISMS resources is therefore defined as a core process of the ISMS (C).

This process is also part of the service management system. While planning the integration of an information security management system with a service management system this enables synergy effects by planning an integrated instead of two separate processes.

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Resource management process	X	X	X	X	X	C

Table 13 – Classification of the resource management process

5.5.5 Process to assure necessary awareness

The process to assure necessary awareness consists of development and implementation of an information security awareness, training and education program. Objectives of the process are to ensure that all personnel receives the necessary security training and/or education. Employees shall be aware of the information security policy, their contribution to the effectiveness of ISMS including the benefits of improved information security performance and implications of not conforming with ISMS requirements.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – Yes

While the process is designed in the ISMS planning process it is carried out while operating the ISMS by an information security training team as part of the ISMS-Team. Often controls or changed controls are accompanied by awareness measures to inform all employees about the changed security controls.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  Necessary knowledge and method skills regarding the assurance information security at a competitive level is only present within the ISMS and because of that the awareness for information security can most efficient and effective be realized within the ISMS.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  As an adequate security awareness is a core element of building an appropriate overall information security level the information security officer is clearly accountable for that.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  Ensuring that all employees have the necessary competence (as part of this process as it is documented in (International Organization for Standardization and International Electrotechnical Commission, 2013)) for doing their work rather seems to be the accountability of the human resources department. Given that in the following this process will be focused at the awareness component of the process. The method skills for ensuring awareness should be present in other departments or functions like human resources, organization department or data protection officer. Necessary knowledge regarding information security at a competitive level is only present within the ISMS and because of that the awareness for information security can most efficient and effective be realized within the ISMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  Well trained and aware employees can act as defined in the policies and standards of the organization and can realize controls as part of the risk treatment in their day to day routine work. In this way the process supports the risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – *Yes*

The process generates a direct value to the management because only well trained and aware employees can act as defined in the policies and standards of the organization to achieve the objectives of the organization.

Classification result

Because all criteria of ISMS core processes to assure necessary awareness is categorized as core process (C).

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Process to assure necessary awareness	X	X	X	X	X	C

Table 14 – Classification of the process to assure necessary awareness

5.5.6 Communication process

The communication processes [10, p. 6] is a part of the broader information risk management process and includes internal and external communication as well as marketing for the ISMS and the reporting regarding information security for customers and the management.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

The communication process as part of the information risk management process is an integral part of the operation of an ISMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  Communication know how and skills must be present within the ISMS to effectively manage information security. Appropriate communication skills are a critical success factor for the ISMS as communication must be ensured with all departments and hierarchical levels.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  While this process is an integral part of an ISMS the owner of the risk communication process is the information security officer because the information security officer is made accountable for achieving the process objective(s) by the top management.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  The method skills for communication are of course present in other departments of the organization. Necessary knowledge about what to communicate regarding information security at a competitive level is only present within the ISMS and because of that the communication regarding information security can most efficient and effective be realized within the ISMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  The process is the core competency of the ISMS as it supports the communication of the results of the core competencies risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

The risk communication process is value generating for the top management while it directly satisfies the information needs of the top management.

Classification result

Because all criteria of ISMS core processes are fulfilled the information security risk assessment process is categorized as core process (C).

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Communication process	X	X	X	X	X	C

Table 15 – Classification of the communication process

5.5.7 Documentation and records control process

Documentation and records control process is the process to identify, create, update and control information determined to be necessary for the effectiveness of the ISMS.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

While processing records and other operational documentation the process is of course operational.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  In practice document management is often not a very welcome task for ISMS staff, but know how and skills regarding the management of documents and records must be present within the ISMS because several regulative documents will be created within the ISMS and a lot of records will be produces while performing the ISMS processes.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  To appropriately manage documentation and records is a responsibility of the information security officer because this documentation enables him to provide evidence of an appropriate ISMS.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  In all other departments or management systems of the organization documents and records must be managed too. So skills and knowhow will be widely spread throughout the organization and should be centralized in an overall documents and records management process. But often this centralized documents and records management is not present. Because of the limited scope of this process regarding the document and records management within the ISMS, the management of information determined to be necessary for the effectiveness of the ISMS should be performed within the ISMS to ensure effectiveness and efficiency.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  As the processes risk assessment and risk treatment produce documents and records and at the same time rely on the availability of relevant documents and records this process supports the risk management and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – *Yes*

Providing access to information necessary to proof an appropriate ISMS seems not to be a direct value delivery to the stakeholders. But ensuring an appropriate documentation and records enables achieving the maturity level "defined" and is a prerequisite of further maturity levels. Having an ISMS with a defined maturity level in place could be a direct value for the stakeholders. Providing access to information necessary to proof an appropriate ISMS is also a direct value for the information security officer because he is responsible to proof an appropriate ISMS to the top management. Furthermore well managed documents with the use of the documentation and records control and the communication process enables the employees to have access to relevant ISMS documents which will lead to a higher security level.

Classification result

Because all criteria of ISMS core processes are fulfilled the documentation control process is categorized as core process (C).

This process is also part of the service management system. While planning the integration of an information security management system with a service management system this enables synergy effects by planning an integrated instead of two separate processes.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Documentation and records control process	X	X	X	X	X	C

Table 16 – Classification of the documentation and records control process

5.5.8 Requirements management process

Requirements management process is the process to ensure an up-to-date understanding of the needs and expectations of interested parties relevant to information security and the ISMS.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

Identifying information security requirements is performed while operating the ISMS as requirements are changing regularly – sometimes even a daily basis – and the changed requirements must be considered within the ISMS and the ISMS processes.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  An up-to-date understanding of the needs and expectations of interested parties relevant to information security and the ISMS is necessary to ensure he appropriateness of the ISMS. Also in the processes risk assessment and risk treatment requirements play an important role to identify risks and risk mitigation options.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  The identification of all relevant requirements for information security is the responsibility of the information security officer.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  Outside the ISMS method skills to identify requirements should be present in an overall requirements management process but an up-to-date understanding of the needs and expectations of interested parties relevant to information security and the ISMS is best realized within the ISMS as there is also a competitive expert know how regarding information security present.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  An up-to-date understanding of the needs and expectations of interested parties relevant to information security and the ISMS plays an important role in the processes risk assessment and risk treatment to identify risks and appropriate risk mitigation options.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

Identified and assigned requirements is a prerequisite to generate a direct value to the stakeholders. From the perspective of the ISMS having an up-to-date and assigned list of relevant requirements is key to implement and maintain an appropriate information security level. So this is a direct value from the perspective of the ISMS and its stakeholders.

Classification result

Because all criteria of ISMS core processes are fulfilled the requirements management process is categorized as core process (C).

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Requirements management process	X	X	X	X	X	C

Table 17 – Classification of the requirements management process

5.5.9 Information security change management process

Information security change management is the process to control changes of ISMS elements and review the consequences of unintended changes. This process only focusses on change management of the ISMS.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – Yes

Changes occur at all levels – strategic, tactic and operational. As a nature of operational changes the most changes occur at an operational level. So the change management process is mainly an operational process.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – Yes

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  Changes occur in all departments and management systems in an organization. So change management is also included in the ISMS which means that the necessary skills and know how to manage changes must be present within the ISMS.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  Taking into account the focus of this change management process on changes of ISMS elements the information security officer should be the owner of this process.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  In every organization should be an overall change management process in place. So a competitive know how and skills should also be present outside the ISMS. Taking into account the division of labor the changes within the ISMS should be managed by the ISMS itself. Additionally changes within the ISMS can be managed most efficient and effective within the ISMS as specialized and in depth know how are present only within the ISMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  As an up-to-date understanding of the needs and expectations of interested parties relevant to information security and the ISMS plays an important role in the processes risk assessment and risk treatment to identify risks and appropriate risk mitigation options, changed requirements will also often affect the ISMS itself. An ISMS is not a fixed management system. It needs to be adapted to changed requirements to be effective and efficient and to ensure an efficient and effective risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

While every change managed by the change management process is intended to improve or maintain the information security level of the organization and information security has a direct positive impact on the business of the organization (Nofer, Hinz, Muntermann, & Rossnagel, 2014) the change management clearly provide an direct value for the stakeholders.

Classification result

Because all criteria of ISMS core processes are fulfilled the change management process is categorized as core process (C).

This process is also part of the information security management processes of the service management system (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 18,19). While planning the integration of an information security management system with a service management system this enables synergy effects by planning an integrated instead of two separate processes.

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Information security change management process	X	X	X	X	X	C

Table 18 – Classification of the information security change management process

5.5.10 Process to control outsourced services

The process to control outsourced services is the process, which ensures that information provided to external service providers are processed in compliance with the information security requirements of the outsourcing organization.

This is mainly achieved by analyzing drafts or final contracts if security requirements are met and the development of requests for changes regarding requirements stipulated in contracts as well as planning and executing service provider audits regarding compliance with information security requirements.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

The process to control outsourced services is focused on ensuring information security it is a specialized part of the broader management of providers. The management of providers also includes quality- and performance management (monitoring of key performance indicators), SLA-management and contract management as defined in the supplier management process of the ISO/IEC 20000. Due to the specialization of the process to control outsourced services this process is carried out while operating the ISMS

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  Necessary knowledge and method skills regarding the control of outsourced services, focused on ensuring information security, is only present within the ISMS at a competitive level and because of that it can most efficient and effective be realized within the ISMS.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  The process to control outsourced services is focused on ensuring information security it is a specialized part of the broader management of providers. Therefore, the owner of this specialized process should be the information security officer.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  Where method skills regarding the control of outsourced services are also present in a broader management of providers necessary in-depth knowledge regarding the control of outsourced services, focused on ensuring information security, is only present within the ISMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  The control of outsourced services, focused on ensuring information security, supports the treatment of risk incorporated in the outsourced services and enables to identify risks regarding the outsourcing of services – for example within provider audits. So this process supports risk assessment as well as risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

Like the general management of information security this process ensures an adequate level of information security and is therefore value generating.

Classification result

This process is also part of the service management system (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 18,19). While planning the integration of an information security management system with a service management system this enables synergy effects by planning an integrated instead of two separate processes for supplier management and the control of outsourced processes. Because all criteria of ISMS core processes are fulfilled the process is categorized as core process (C).

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Process to control outsourced services	X	X	X	X	X	C

Table 19 – Classification of the process to control outsourced services

5.5.11 Performance evaluation process

The performance evaluation process (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 7,8) contains monitoring (the performance of ISMS need to be monitored in terms of verification and reporting of security control implementation), measurement (a measurement system to evaluate performance in information security management and feedback suggestions for improvement need to be established (International Organization for Standardization and International Electrotechnical Commission, 2014, p. 11)), analysis and evaluation.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

According to (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 63) the measurement process should be integrated into the ISMS cycle. So it is clearly a part of the ISMS and performed while operating the ISMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  The seamlessly integration of this process in the ISMS cycle requires that necessary know how and skills are present within the ISMS.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  While this process is performed within the operation of the ISMS the information security officer should be owner of this process.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  This process is also part of the service management system [61, p. 16] where it is used to monitor trends and performance against service targets. While planning the integration of an information security management system with a service management system this enables synergy effects by planning an integrated instead of two separate performance evaluation processes. Taking into account the division of labor the performance of the ISMS processes should be managed by the ISMS itself. Additionally the performance management of ISMS processes can be operated most efficient and effective within the ISMS as specialized and in depth know how are present only within the ISMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  Performance evaluation is one of the critical success factors of the ISMS (International Organization for Standardization and International Electrotechnical Commission, 2014, p. 11). In this way it clearly supports risk assessment and risk treatment because without an appropriate performance management this processes cannot be performed efficiently.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

Results of this process like management reports are a direct value for the top management (stakeholders) as it supports decision making of the top management (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 63) regarding ISMS-related decisions and improvement of the ISMS (International Organization for Standardization and International Electrotechnical Commission, 2010b, p. vii).

Classification result

Because all criteria of ISMS core processes are fulfilled the process is categorized as core process (C).

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Performance evaluation process	X	X	X	X	X	C

Table 20 – Classification of the performance evaluation process

5.5.12 Internal audit process

The internal audit process is the process of planning and conducting internal audits as part of an audit program (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 8).

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – Yes

Internal audits regarding information security controls are an integral part of the check phase in the plan-do-check-act cycle of the ISMS. Like the measurement process the internal audit process should be integrated into the ISMS. So it is clearly a part of the ISMS and performed while operating the ISMS

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – Yes

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  The seamlessly integration of this process in the ISMS cycle requires that necessary know how and skills are present within the ISMS.

- Is the process managed or even owned by the ISMS / the information security officer? – Partially

  While this process is performed within the operation of the ISMS the information security officer could be owner of this process. But to ensure reliable and independent results this process should be divided in

  - Internal audit of information security controls - for which the information security officer is the owner.
  - Internal audit of ISMS-processes - for which the top management is the owner.

  This differentiation is necessary because independence is the key criteria which differentiates the internal audit process from the performance evaluation process (measurement and monitoring). Therefore in the following the internal audit process contains only the internal audit of information security controls.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  This process is also part of the service management system (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 18,19). While planning the integration of an information security management system with a service management system this enables synergy effects by planning an integrated instead of two separate processes.

  Where method skills regarding internal audits are also present in a broader management of internal audits and revisions the necessary in-depth knowledge regarding information security controls, is mostly present within the ISMS. Given that, the audit of information security controls can be operated most efficient and effective within the ISMS. Taking into account also the division of labor the internal audit of information security controls should be managed by the ISMS itself.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  The internal audit of information security controls, supports the treatment of risk as it ensures the effectiveness of that controls and enables the identification of additional or overlooked risks. Therefore, this process supports risk assessment as well as risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

Results of this process like audit and management reports are a direct value for the top management (stakeholders) as it supports decision making of the top management (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 63) regarding ISMS-related decisions and improvement of the ISMS (International Organization for Standardization and International Electrotechnical Commission, 2010b, p. vii)

Classification result

As the process is divided in two parts as described above in the following only the part of internal audit of information security controls is defined as the scope of the internal audit process. The part of internal audit of ISMS-processes should be included in an overall internal audit process and the results of that need to be considered in the information security governance process. Because of that differentiation and the fact that the remaining process fulfills all criteria of ISMS core processes process is categorized as core process (C).

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Internal audit process	X	X	X	X	X	C

Table 21 – Classification of the internal audit process

5.5.13 Information security governance process

Information security governance from a holistic perspective is required to cultivate an acceptable level of information security culture and minimizing information security risks (Veiga & Eloff, 2007).

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – No

The information security officer is operationally involved in the process with compiling and presenting management reports. This process is carried out to govern the ISMS. Therefore, it is not a process of the operationally level.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *No*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – No

  While the top management reviews and decides relevant aspects skills and know-how regarding this process are not present within the ISMS because the ISMS can't govern himself.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  The owner of this process is the top management, as they are responsible to initiate the review process and to provide objectives and requirements to manage the ISMS. With the information security governance process objectives for the ISMS are defined and the achievement of the information security objectives are monitored at a general level.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  While the top management reviews and decides relevant aspects skills and know-how regarding this process are not present within the ISMS because the ISMS can't govern itself. The top management has competitive know how to perform this process.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – No

  As objectives for the ISMS are defined as well as the achievement of the information security objectives are monitored at a general level this process influence the risk assessment and risk treatment but does not support them directly.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – *Yes*

Results of this process like informed and efficient management decisions are a direct value for the top management (stakeholders) as it ensures that the ISMS is operated as intended by the top management and will achieve the objectives of the top management.

Classification result

Because not all criteria are fulfilled this process is not an ISMS core process. Because objectives for the ISMS are defined as well as the achievement of the information security objectives are monitored at a general level this process is categorized as a management process.

This process is also part of the service management system. While planning the integration of an information security management system with a service management system this enables synergy effects by planning an integrated instead of two separate processes.

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Information security governance process	X	X	-	-	X	M

Table 22 – Classification of the information security governance process

5.5.14 Information security incident management process

The information security incident management process is for detecting, reporting, assessing, responding to, dealing with and learning from information security incidents.

The objective of this process is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 20).

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

Information security incident management process (active prevention and detection of information security incidents) is a success factor of an ISMS (International Organization for Standardization and International Electrotechnical Commission, 2014, p. 7,11) and part of an operational ISMS (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 31).

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  While this process is an integral part and success factor of an ISMS the necessary know how and skill to perform the ISMS must be present within the ISMS.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  While this process is an integral part of an ISMS the manager of the information security incident management process is the information security officer because the information security officer is made responsible for dealing with and communication of information security incident by the top management.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  In general methodical know how and skill regarding this process will be present within the broader processes of incident management. The processes of incident management and information security incident management have interfaces as information security incidents are a special form of incidents. Nevertheless information security incidents can be operated most efficient and effective within the ISMS as specialized and in depth know how are present only within the ISMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  As occurring information security incidents are input to the risk assessment for identification of risks as wells as the assessment of the likelihood of risks and information security incidents allow to assess the effectiveness of the chosen treatment options this process supports both, risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

The information security incident management process is value generating because security incidents have negative impact on trust in the organization and trust in the organization has a positive consumer impact (Nofer et al., 2014). Also the top management has a direct benefit from the process resulting from the reduction of information security risks (International Organization for Standardization and International Electrotechnical Commission, 2014, p. 11).

Classification result

As all requirement are fulfilled this process is categorized as an ISMS core process.

This process is also part of the service management system (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 18,19). While planning the integration of an information security management system with a service management system this enables synergy effects by planning an integrated instead of two separate processes.

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Information security incident management process	X	X	X	X	X	C

Table 23 – Classification of the Information security incident management process

5.5.15 Service level management process

The service level management process is the process to define, agree, record, and manage levels of services (International Organization for Standardization and International Electrotechnical Commission, 2012b, p. 8). The service level management process should ensure that the service provider remains focused on the customer throughout the planning, implementation, and ongoing management of service delivery. The service provider shall agree a catalogue of services with the customer and for each service delivered, one or more service level agreements shall be agreed with the customer (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 15).

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *No*

This process is performed in the operational phase of the service management system (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 15) and not while operating the ISMS. So it is operational, but not part of the ISMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *No*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are not present within the ISMS at a competitive level.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the accountability lies within manager of the service management system.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are present within the SMS at a competitive level. So this process is performed most effective and efficient by the SMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – No

  This process does not support the two identified core competencies risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

Of course the service level management process is value generating because it is the aim of this process to align provided services with the customer needs.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process is classified to belong to another management system.

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Service level management process	X	X	-	-	X	O

Table 24 – Classification of the service level management process

5.5.16 Service reporting process

The objective of the service reporting process is to produce agreed timely, reliable, accurate reports for informed decision making and effective communication regarding the services.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – No

This process is performed in the operational phase of the service management system (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 15) and not while operating the ISMS. So it is operational, but not part of the ISMS. It could be argued that service reporting is also necessary within an ISMS as the ISMS also delivers services to its customers. But an ISMS specific version of this process is already integrated in the "communication process". So this process of service reporting clearly belongs to the SMS and not to the ISMS but synergy effects can be used for this processes when integrating an ISMS and a SMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – No

- Are the necessary know how and skills present in the ISMS to perform the process very well? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are not present within the ISMS at a competitive level.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the accountability lies within manager of the service management system.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are present within the SMS at a competitive level. So this process is performed most effective and efficient by the SMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – No

  This process does not support the two identified core competencies risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

The service reporting process is value generating because it enables informed decisions of the service provider.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process is classified to belong to another management system.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Service reporting process	X	X	-	-	X	O

Table 25 – Classification of the Service reporting process

5.5.17 Service continuity and availability management process

The service continuity and availability management process is the process to ensure that agreed service continuity and availability commitments to customers can be met in all circumstances. The service continuity and availability management process consists of the identification of service continuity and availability requirements, creating, implementing and maintaining a service continuity plan and an availability plan as well as service continuity and availability monitoring and testing (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 16,17).

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *No*

This process is performed in the operational phase of the service management system (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 15) and not while operating the ISMS. So it is operational, but not part of the ISMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Partially*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are not present within the ISMS at a competitive level.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  From the viewpoint of the ISMS continuity and availability plans are part of the measures chosen in the risk treatment process. Those plans are not created implemented or maintained in the ISMS, but in the service management system. So the accountability for this process lies within manager of the service management system.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are present within the SMS at a competitive level. So this process is performed most effective and efficient by the SMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  While availability of information is one objective of the ISMS the availability requirements of services are input for the information security risk assessment process. So process interfaces for these processes should be defined. From the viewpoint of the ISMS continuity and availability plans are part of the measures chosen in the risk treatment process.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

The process supports meeting the customer requirements which is of direct value for the customers.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process is classified to belong to another management system.

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Service continuity and availability management process	X	X	-	(X)	X	O

Table 26 – Classification of the Service continuity and availability management process

5.5.18 Budgeting and accounting for services process

In the budgeting and accounting for services process direct and indirect costs for services are identified to enable an effective financial control and approval.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – No

This process provides input to the change management process in the service management system and so it belongs to the SMS and not to the ISMS.

But this process is comparable with the resource management process of the ISMS which is also linked with the information security change management process via the information security risk treatment process. Both processes offer synergy effects while integrated into a single process. At least interfaces between those processes should be established to enable an overall cost control of services including information security measures.

Like the change management process the budgeting and accounting for services process need to be performed operationally when changes are planned because regular monitoring and reporting of costs is also part of this process (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 17).

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Partially*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  Planning of budgets and cost control are relevant in the ISMS as well as in the SMS. So in both management systems appropriate know how and skills must be present at a comparable level.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  Because planning of budgets and cost control for services are core aspects of the service management, the accountability for this process lies within the manager of the service management system. If integrated into a single process with the resource management process accountability of this integrated process should stay in the service management because information security costs – indirect ISMS-costs as well as costs for service specific security measures – are part of the costs assigned to services.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  Planning of budgets and cost control are relevant in the ISMS as well as in the SMS. So in both management systems appropriate know how and skills must be present at a comparable level.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Partially

  This process is comparable with the resource management process of the ISMS which is also linked with the information security change management process via the information security risk treatment process. Planning of budgets and cost control is also relevant when planning risk treatment options. So it partially supports the two identified core competencies risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – *Yes*

Cost control is a direct value for the customers of services because they also have no unlimited resources or budgets.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process is classified to belong to another management system.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Budgeting and accounting for services process	X	X	-	(X)	X	O

Table 27 – Classification of the budgeting and accounting for services process

5.5.19 Capacity management process

The capacity management process consists of the identification and agreement of capacity and performance requirements with the customer and interested parties (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 18).

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *No*

This process is performed in the operational phase of the service management system (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 18) and not while operating the ISMS. So it is operational, but not part of the ISMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Partially*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are not present within the ISMS at a competitive level.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  From the viewpoint of the ISMS capacity planning is part of the measures chosen in the risk treatment process. Those plans are not created implemented or maintained in the ISMS, but in the service management system. So the accountability for this process lies within manager of the service management system.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are present within the SMS at a competitive level. So this process is performed most effective and efficient by the SMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Partially

  From the viewpoint of the ISMS capacity planning is part of the measures chosen in the risk treatment process. Therefore, it partially support the risk treatment process. But those plans are not created implemented or maintained in the ISMS, but in the service management system.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

The process supports meeting the customer requirements, which is of direct value for the customers.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process is classified to belong to another management system.

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Capacity management process	X	X	-	(X)	X	O

Table 28 – Classification of the capacity management process

5.5.20 Business relationship management process

The business relationship management process consists of the following (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 19,20):

- identification and documentation of the customers, users and interested parties
- establishment of a communication mechanism with the customers
- documentation of a procedure to manage service complaints from the customers
- measurement of the customer satisfaction at planned intervals
- Initiation of changes in the SLA or the service requirements

The business relationship management provides various input for other processes like the service management process, the change management process, and improvement processes.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *No*

The business relationship management process need to be performed at an operational level, because complaints and changes need to be considered in the operation of the services. This process is performed in the operational phase of the service management system (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 18) and not while operating the ISMS. So it is operational, but not part of the ISMS.

It could be argued that information security customer relationship management is also necessary within an ISMS and this is not integrated in the processes identified from ISO 27001. This special version of the business relationship management process is discussed separately in chapter 5.5.28 Information security customer relationship management.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Partially*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are not present within the ISMS at a competitive level.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the accountability lies within manager of the service management system.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are present within the SMS at a competitive level. So this process is performed most effective and efficient by the SMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Partially

  As the business relationship management process identifies the customers, users and interested parties, establish a communication mechanism with the them and measures their satisfaction this process helps to identify requirements (which is necessary within the risk identification) and supports the communication of risks (which supports the communication process). So this process partially supports risk assessment and risk treatment if information security is understood as a service.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

The business relationship management process is value generating as it ensures an appropriate customer satisfaction.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process is classified to belong to another management system.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Business relationship management process	X	X	-	(X)	X	O

Table 29 – Classification of the business relationship management process

5.5.21 Supplier management process

Processes operated by other parties need to be governed (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 8). The supplier management process mainly consists of (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 20,21):

- Defining a designated individual who is responsible for managing the relationship, the contract and performance of the supplier
- Defining a contract
- Planning and executing performance monitoring

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *No*

Information security is one aspect of the supplier management which is not especially mentioned in the ISO/IEC 20000. This process is linked with the ISMS process to control outsourced services but it is performed in the operational phase of the service management system. So it is operational, but not part of the ISMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Partially*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Partially

  This process is part of the service management system and it is not mentioned in the information security management system. But as information security is one aspect of the supplier management the necessary skills and know how needed to perform that process are partially present within the ISMS.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  Information security is one aspect of the supplier management which is not especially mentioned in the ISO/IEC 20000. This process is linked with the ISMS process to control outsourced services, but the accountability for this general supplier management process lies within manager of the service management system.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Partially

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are present within the SMS at a competitive level. So this process – except the aspect of information security – is performed most effective and efficient by the SMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – No

  As this process does not focus on information security it does not support the two identified core competencies risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

So the process supports meeting the service level agreements when processes or parts of them are outsourced which is of direct value for the customers.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process is classified to belong to another management system.

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Supplier management process	X	X	-	(X)	X	O

Table 30 – Classification of the supplier management process

5.5.22 Incident and service request management

The incident and service request management process focusses on incidents and service requests which should be managed by the same process (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 21). So the classification of the incident management part is identical to the incident management process from ISO 27001. Given that in the following only the service request management part of that process will be discussed. The service request management process focus on managing the fulfilment of service requests from recording to closure.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – No

This process is performed in the operational phase of the service management system and not while operating the ISMS. So it is operational, but not part of the ISMS. It could be argued that service requests regarding ISMS services are also necessary within an ISMS as the ISMS also delivers services to its customers. But an ISMS specific version of this process is already integrated in the "requirements management process". So this process of service request management mainly belongs to the SMS and not to the ISMS but synergy effects can be used for this processes when integrating an ISMS and a SMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – Partially

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Partially

  As this general service request management process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are only present within the ISMS as it is necessary to process requirements of customers in the requirements management process.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  While the accountability for the management of service requests should stay in the service management system, information security incidents should be managed in the ISMS. So the accountability of an integrated incident and service request management process could be assigned to manager of the ISMS or the SMS. But as mentioned above the discussion here does focus on the service request management part, which should be managed within the SMS.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are present within the SMS at a competitive level. So this process is performed most effective and efficient by the SMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – No

  This process does not support the two identified core competencies risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

As this process ensures that customer service requests are processed and fulfilled the process is value generating.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process is classified to belong to another management system.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Incident and service request management process	X	X	-	(X)	X	O

Table 31 – Classification of the incident and service request management process

5.5.23 Problem management process

The problem management process focusses on the analyzation of data and trends on incidents and problems to identify root causes and their potential preventive action (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 22). Up-to-date information on known errors and problem resolutions will be provided to the incident and service request management process as output of this process.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – No

This process is performed in the operational phase of the service management system and not while operating the ISMS. So it is operational, but not part of the ISMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – Partially

- Are the necessary know how and skills present in the ISMS to perform the process very well? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are not present within the ISMS at a competitive level.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the accountability lies within manager of the service management system.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are present within the SMS at a competitive level. So this process is performed most effective and efficient by the SMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  This process should be linked to the risk assessment and risk treatment process as it provides input regarding root causes to identify and understand risks as well as to identify measures (changes) to prevent further occurrence of risk events/incidents.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

This process is value generating as it prevents further occurrence of incidents and the realization of risks.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process is classified to belong to another management system.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Problem management process	X	X	-	(X)	X	O

Table 32 – Classification of the problem management process

5.5.24 Configuration management process

The configuration management process ensures that every configuration item including their relationships to other configuration items and service components is uniquely recorded in the configuration management database (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 22,23) which is used as input for most operational ISMS and SMS processes.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – No

Ensuring the actuality of the configuration management database requires that this process is performed at an operational level. So this process is performed in the operational phase of the service management system and not while operating the ISMS. It is operational, but not part of the ISMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – Partially

- Are the necessary know how and skills present in the ISMS to perform the process very well? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are not present within the ISMS at a competitive level.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the accountability lies within manager of the service management system.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  As this process is part of the service management system and it is not mentioned in the information security management system the necessary skills and know how needed to perform that process are present within the SMS at a competitive level. So this process is performed most effective and efficient by the SMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  As a reliable, actual and correct configuration management database provides significant data necessary to perform risk assessment and risk treatment this process supports the two identified core competencies risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – No

This process ensures that every configuration item including their relationships to other configuration items and service components is uniquely recorded in the configuration management database (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 22,23) which is used as input for most operational ISMS and SMS processes. So this process is not of a direct value for the customers and other stakeholders of the ISMS and SMS, but it supports the value generation of other processes.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process should be classified to belong to another management system. But considering the importance of the output of this process for risk assessment and risk treatment this process is classified as “support process”.

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Configuration management process	X	X	-	(X)	-	S

Table 33 – Classification of the configuration management process

5.5.25 Change management process

Where the information security change management is the process to control changes of ISMS elements and review the consequences of unintended changes, the change management process of the SMS focusses on changes of CIs, service components and services.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – Yes

As a nature of operational changes the most changes occur at an operational level. So the change management process is mainly an operational process.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – Partially

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  Changes occur in all departments and management systems in an organization. So change management is also included in the ISMS which means that the necessary skills and know how to manage changes must be present within the ISMS

- Is the process managed or even owned by the ISMS / the information security officer? – No

  Taking into account the focus of this change management process on changes of CIs, services and service components the manager of the SMS should be the owner of this process.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  In every organization should be an overall change management process in place and a specialized information security change management process is also in place. So a competitive know how and skills should also be present within the ISMS. But taking into account the division of labor changes to CIs, service components and services should be managed by the SMS itself. Additionally changes within the SMS can be managed most efficient and effective within the SMS as specialized and in depth know how are present only within the SMS.

  Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  The change management process ensures a reliable, actual and correct configuration management database. As a reliable, actual and correct configuration management database provides significant data necessary to perform risk assessment and risk treatment this process supports the two identified core competencies risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

While every change managed by the change management process is intended to improve or maintain the service level it has a direct positive impact on the business of the organization and so the change management clearly provide a direct value for the stakeholders.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process should be classified to belong to another management system.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Change management process	X	X	X	(X)	X	O

Table 34 – Classification of the change management process

5.5.26 Release and deployment management process

The release and deployment management process is used to deploy approved new or changed services into the live environment (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 15) so that the integrity of hardware, software and other service components is maintained during deployment of the release. Planning includes the dates for deployment of each release, deliverables and methods of deployment (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 24).

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

Changes occur at all levels – strategic, tactic and operational. As a nature of operational changes the most changes including emergency changes occur at an operational level. So the deployment management process is also mainly an operational process.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *No*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – No

  Necessary know how and skills to manage and deploy releases are not present within the ISMS, but within the SMS.

- Is the process managed or even owned by the ISMS / the information security officer? – No

  Taking into account the focus of this release and deployment management process on changes of CIs, services and service components the manager of the SMS should be the owner of this process.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – No

  Necessary know how and skills to manage and deploy releases are not present within the ISMS, but within the SMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – No

  The management and deployment of releases does not directly support risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – *Yes*

While every change – managed by the change management process and deployed within the release and deployment management process – is intended to improve or maintain the service level it has a direct positive impact on the business of the organization and so the release and deployment management process clearly provide a direct value for the stakeholders.

Classification result

As this process is part of the service management system and it is not mentioned in the information security management system and not all ISMS core process criteria are fulfilled this process should be classified to belong to another management system.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Release and deployment management process	X	X	X	-	X	O

Table 35 – Classification of the release and deployment management process

Because of the focus of this process it must also be a core competency of the SMS.

5.5.27 Information security improvement process

The information security improvement process is the process to ensure and improve a continuing suitability, adequacy and effectiveness of the ISMS.

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

This process is performed while operating the ISMS, so it is an operational process.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  As this process is performed while operating the ISMS, necessary know how and skills must be present within the ISMS.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  The information security officer is owner of this process, as he or she is responsible for an effective and efficient ISMS.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  This process is also part of the service management system. While planning the integration of an information security management system with a service management system this enables synergy effects by planning an integrated instead of two separate processes. Because of that methodical know how and skills regarding this process are also present within the SMS. But the necessary knowledge regarding information security at a competitive level is only present within the ISMS and because of that the information security improvement can most efficient and effective be realized within the ISMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  As the processes risk assessment and risk treatment are also target of the information security improvement process this process supports risk assessment and risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

Results of this process like request for changes to improve the ISMS a direct value for the top management (stakeholders) as it ensures that the ISMS is operated effectively and efficiently.

Classification result

While all criteria are met, this process is a core competency of the ISMS.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Information security improvement process	X	X	X	X	X	C

Table 36 – Classification of the information security improvement process

5.5.28 Information security customer relationship management

On the basis of (International Organization for Standardization and International Electrotechnical Commission, 2011, p. 19,20) the information security customer relationship management process consists of the following:

- Identification and documentation of the customers, users and interested parties
- Establishment of a communication mechanism with the customer
- Establish a method for measuring and demonstrating the value of information security and the efficient resource usage (Information Systems Audit and Control Association, n.d.-c, p. 53).
  - Track outcomes of information security initiatives and compare to expectations to ensure value delivery against business goals.
  - Measurement of the customer satisfaction at planned intervals
  - Establish and documented procedure to manage information security complaints from the customer
- Initiation of changes to improve the customer satisfaction
- Communicate information security performance and added value to the customers

ISMS core process criteria 1 – Operational – Is the process carried out while operating the ISMS? – *Yes*

This process need to be performed at an operational level, because complaints and changes need to be considered while operate the ISMS.

ISMS core process criteria 2 – Core competency – Is the process a core competency of the ISMS and the information security officer is the process owner or process manager? – *Yes*

- Are the necessary know how and skills present in the ISMS to perform the process very well? – Yes

  As complaints and changes need to be considered while operate the ISMS necessary skills and know how must be present within the ISMS.

- Is the process managed or even owned by the ISMS / the information security officer? – Yes

  To continuously demonstrate the added value of the ISMS or information security controls is the responsibility of the information security officer, who should therefore be the owner of this process.

- Does no one elsewhere in the organization have a competitive know how and skills to perform the process more efficient and/or effective as the ISMS? – Yes

  Beside general methodical skills, considering complaints and changes regarding the ISMS, information security and information security measures requires specialized know how which is only present within the ISMS.

- Does the competency support the two identified core competencies risk assessment and risk treatment? – Yes

  As every risk treatment option identified within the risk treatment process regarding risks identified in the risk assessment process must demonstrate its value this process supports risk assessment as well as risk treatment.

ISMS core process criteria 3 – Value generating – Does the process deliver apparent and direct value to the stakeholder? – Yes

According to the COBIT process EDM02 (Information Systems Audit and Control Association, n.d.-c, p. 73) – ensure benefits delivery – it is also necessary for information security to ensure an appropriate balance between benefits, and costs of information security investments as well as risks. This is especially necessary as most costs for information security controls are funded by or charged to the demanding customers. Financial and non-financial measures are used to describe the added value of information security management.

Of course the business relationship management process is value generating as it ensures an appropriate customer satisfaction.

Classification result

While all criteria are met, this process is a core competency of the ISMS.

Process/criteria	General process criteria		ISMS core process criteria			Resulting category-zation
	Regula-rity	Transfor-mation	Opera-tional	Core com-petency	Value generating	
Information security customer relationship management process	X	X	X	X	X	C

Table 37 – Classification of the information security customer relationship management process

5.6 ISMS process framework

This part of chapter 5 contains the result of the discussion of the former part of this chapter illustrated in a process framework. This represents the concluded answer to MRQ1-4 "What is the agreed basis of ISMS processes in existing standards and in the latest ISMS process research work?" The following Table 38 – Matching ISMS core process criteria against identified ISMS processes contains the result of matching the identified ISMS processes against the criteria for ISMS core processes.

- **"X"** indicates that the process fulfills the criteria.
- **"(X)"** indicates that the process partially fulfills the criteria.
- **"-"** indicates that the process does not fulfill the criteria.
- **"M"** is used for indicating management processes of the information security management system.
- **"C"** is used for indicating core processes of the information security management system.
- **"S"** is used for indicating support processes of the information security management system.
- **"O"** is used for indicating that the process belongs to another management system.

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Trans-forma-tion	Opera-tional	Core compe-tency	Value gene-rating	
ISMS planning process (project) – see chapter 5.5.1	-	X	-	(X)	X	project
Information security risk assessment process - 5.5.2	X	X	X	X	X	C
Information security risk treatment process - see chapter 5.5.3	X	X	X	X	X	C
Resource management process - see chapter 5.5.4	X	X	X	X	X	C
Process to assure necessary awareness and competence - see chapter 5.5.5	X	X	X	(X)	X	C
Communication process - see chapter 5.5.6	X	X	X	X	X	C
Documentation and records control process - see chapter 5.5.7	X	X	X	X	X	C
Requirements management process - see chapter 5.5.8	X	X	X	X	X	C
Information security change management process - see chapter 5.5.9	X	X	X	X	X	C
Process to control outsourced services - see chapter 5.5.10	X	X	X	X	X	C

Process/criteria	General criteria	process	ISMS core process criteria			Resulting category-zation
	Regula-rity	Trans-forma-tion	Opera-tional	Core compe-tency	Value gene-rating	
Performance evaluation process - see chapter 5.5.11	X	X	X	X	X	C
Internal audit process - see chapter 5.5.12	X	X	X	X	X	C
Information security governance process - see chapter 5.5.13	X	X	-	-	X	M
Information security incident management process - see chapter 5.5.14	X	X	X	X	X	C
Service level management process - see chapter 5.5.15	X	X	-	-	X	O
Service reporting process - see chapter 5.5.16	X	X	-	-	X	O
Service continuity and availability management process - see chapter 5.5.17	X	X	-	(X)	X	O
Budgeting and accounting for services process - see chapter 5.5.18	X	X	-	(X)	X	O
Capacity management process - see chapter 5.5.19	X	X	-	(X)	X	O
Business relationship management process - see chapter 5.5.20	X	X	-	(X)	X	O
Supplier management process - see chapter 5.5.21	X	X	-	(X)	X	O
Incident and service request management process - see chapter 5.5.22	X	X	-	(X)	X	O
Problem management process - see chapter 5.5.23	X	X	-	(X)	X	O
Configuration management process - see chapter 5.5.24	X	X	-	(X)	-	S
Change management process - see chapter 5.5.25	X	X	X	(X)	X	O
Release and deployment management process - see chapter 0	X	X	X	-	X	O
Information security improvement process - see chapter 5.5.27	X	X	X	X	X	C
Information security customer relationship management process - see chapter 5.5.28	X	X	X	X	X	C

Table 38 – Matching ISMS core process criteria against identified ISMS processes

ISMS processes and their interaction at a high level basis are shown in Figure 7 – ISMS process framework.

This ISMS processes must be individually integrated into existing management systems and processes. This is not displayed in the figure to ensure readability and because existing management systems differ too much in praxis. As a first starting point for the integration towards an integrated management system the detailed process descriptions or the detailed process flowcharts of Appendix B – Process Profiles in addition to the established or agreed other process frameworks like (International Organization for Standardization and International Electrotechnical Commission, 2011) should be used.

As every ISMS process provides input for the documentation and records control process and the ISMS planning process provides input for every ISMS process those interfaces are not displayed in the process charts to enable a better readability of Figure 7 – ISMS process framework.

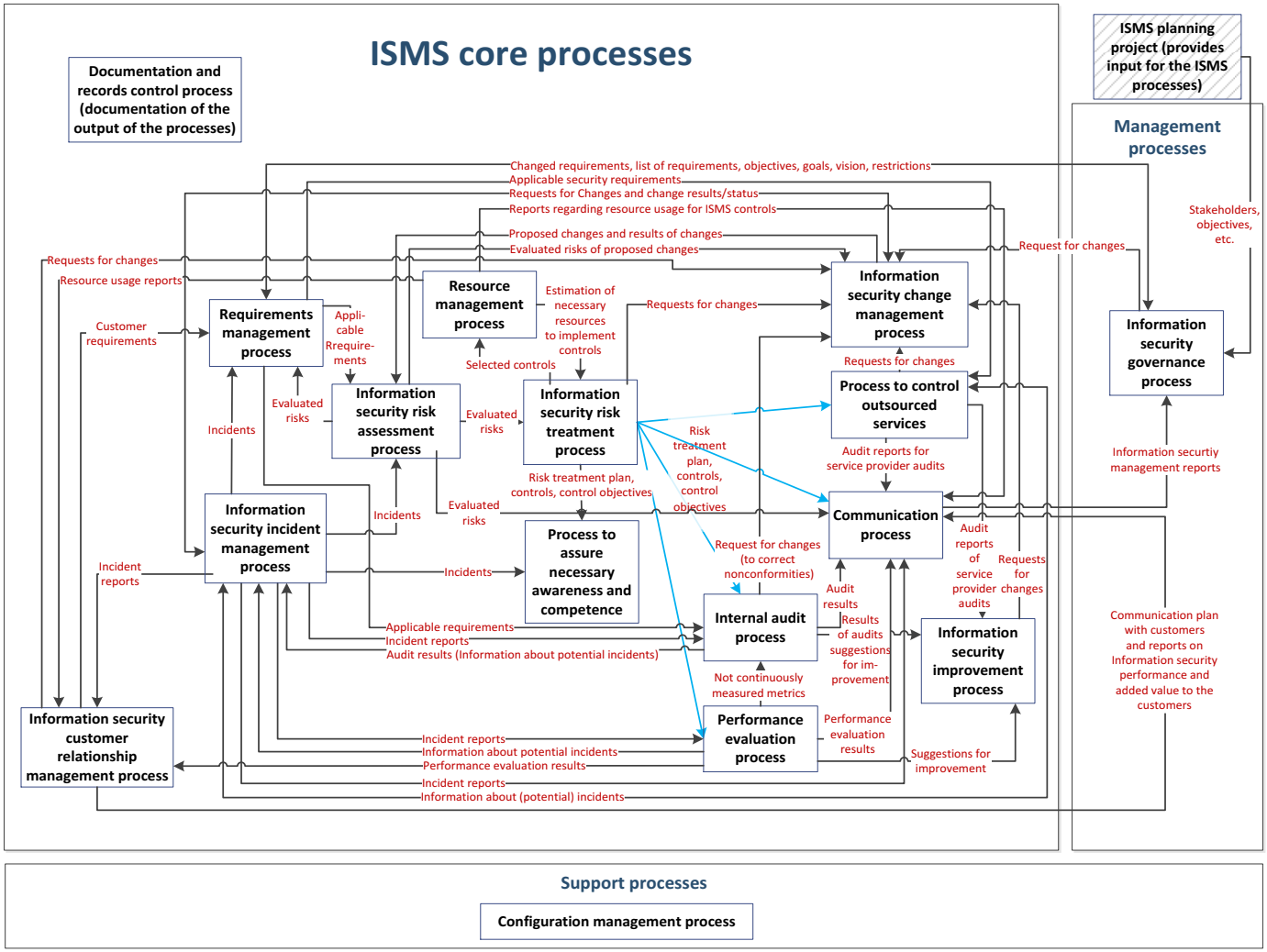

Figure 7 – ISMS process framework

As every ISMS process provides input for the documentation and records control process and the ISMS planning as well as the configuration management process provides input for every ISMS process those interfaces are not illustrated to enable a better readability of Figure 7 – ISMS process framework.

The **ISMS planning process** is the process of ISMS specification and design from inception to the production of implementation plans. **Documentation and records control process** is the process to identify, create, update and control information determined to be necessary for the effectiveness of the ISMS.

Key to reach the ISMS objectives is an up-to-date understanding of the needs and expectations of interested parties relevant to information security and the ISMS. This is realized within the **requirements management process**, which provides identified legal, statutory, regulatory and contractual requirements for the risk assessment process, the internal audit process and the process to control outsourced processes.

In the **risk assessment process**, risks are identified, analyzed and evaluated. The output of this process are documented and evaluated risks in a list of prioritized risks including threats, vulnerabilities and risk owners, consequences and business impact, likelihood and comparison against risk criteria as well as evaluated risks of proposed changes, which are input for the communication process and the information security risk treatment process.

In the **information security risk treatment process** risk treatment options including control objectives and controls are identified and selected. Output of this process are list with selected controls and control objectives, a risk treatment plan including acceptance of residual risks, a control implementation plan and requests for changes to information security change management process, which are used as input in various ISMS processes.

To implement the controls as well as to run the ISMS processes resources are needed which are identified, allocated and monitored in the **resource management process**. Output of the resource management process are planned/documented resources to implement and run selected controls, categorization of controls regarding who funds the control, planned and documented resources to run the ISMS core processes, reports regarding resource usage of ISMS core processes, and for the information security customer relationship management process: reports on resource usage. The implementation of controls are always changes, which can be managed within a general change management process of the implementing organization or – if the change focuses on an ISMS element – within the **information security change management process**. The information security change management process is the process to control changes of ISMS elements and review the consequences of unintended changes. This process only focusses on change management of the ISMS. Output of this process are necessary changes (for documentation and records control process), proposed and necessary changes as well as results of changes (for and from risk assessment process), initiation of risk assessment when significant changes are proposed or occur and the results of changes to information security incident management process, as they were initiated by that process.

The **information security incident management process** is for detecting, reporting, assessing, responding to, dealing with and learning from information security incidents. Outputs of this process are identified incidents which are used in various ISMS processes including the information security change management process and the process to ensure necessary awareness and competence.

In the **information security awareness process** an information security awareness, training and education program is developed and implemented to ensure that all personnel receives the necessary security training and/or education.

As services are outsourced, these services need to be determined and controlled, which is realized within the **process to control outsourced services**.

The **performance evaluation process** contains monitoring, measurement, analysis and evaluation of two main criteria. First, the performance of the security controls and second the performance of the ISMS processes. Performance measurement differs from performance audit (internal audit) regarding effectiveness and efficiency of the ISMS and implemented controls which is performed independently within the **internal audit process.**

Results from the performance evaluation process, the internal audit process as well as results from the service provider audits from the process to control outsourced services are used to improve effectiveness, efficiency, suitability and adequacy of the ISMS and the controls. This is realized within the **information security improvement process**.

Results of nearly all ISMS processes are centrally communicated within the **communication process** to stakeholders outside the ISMS. This includes the communication of risks and information security management reports. Those reports as well as identified requirements are input for the **information security governance process**, which ensures an alignment of the ISMS with the objectives and needs of the governing stakeholders.

The information security governance process forms the interface between the ISMS and its stakeholders. Beside this the operational management of the customer satisfaction level as well as the continuous demonstration of the added value of investments in information security needs to be realized. This is done within the **information security customer relationship management process**.

The processes are described in more detail in Appendix B – Process Profiles.

6 Maturity Level Model for ISMS core processes

In chapter 4 State of the art – capability and maturity level models current capability and maturity level models were discussed.

The actual state of the art of ISMS and capability maturity models does not stipulate the use of capability and maturity models while implementing and operating an ISMS. But processes like continuous improvement of the ISMS can be performed using a maturity level model to measure and to demonstrate the improvement. Nevertheless according to (Huang & Han, 2008) ISO standards for ISMS are generally addressing minimum criteria for an ISMS while the CMMI emphasizes improvement in different levels.

A systematic literature review (SLR) / mapping study (Kitchenham et al., 2011) was planned to identify and categorize all relevant research papers related to capability maturity models and their use in ISMS to answer research question MRQ2-1 to MRQ2-3.

The following research questions should be answered by a SLR:

- MRQ2-1: What are criteria for the applicability of maturity models within ISMS?
- MRQ2-2: Are maturity models already used within ISMS?
- MRQ2-3: What is the most appropriate maturity model for the use within ISMS?

In chapter 6.2 SLR – Analysis of the latest research regarding maturity level model use within an ISMS the results of a systematic literature review will be presented to answer the research question MRQ2-2: Are maturity models already used within ISMS?

As a prerequisite, criteria for the applicability of a maturity level model for the use within an ISMS need to be developed to answer the research question MRQ2-1 ”What are criteria for the applicability of maturity models within ISMS?”. Results of this will be presented in chapter 6.1 Criteria for the applicability of a maturity level model for the use within an ISMS.

The results will be the basis for the selection of an appropriate maturity level model to answer the research question MRQ2-3: “What is the most appropriate maturity model for the use within an ISMS?”.

6.1 Criteria for the applicability of a maturity level model for the use within an ISMS

As a prerequisite, criteria for the applicability of a maturity level model for the use within an ISMS was planned to be developed within an systematic literature analysis to answer the research question MRQ2-1 ”What are criteria for the applicability of maturity models within ISMS?” After that the identified criteria for the applicability of a maturity level model for the use within an ISMS will be applied to the relevant maturity level models.

For this thesis it is obvious that:

- A main criteria is, that the maturity level model should fit for all organizations independent of their size, objectives, business model, location et cetera.
- A second main criteria is that the maturity level model is internationally accepted and enables an international acceptance of the later developed method to determine the necessary maturity level.

This obvious criteria already suitably answers MRQ2-1 and therefore an SLR regarding this research question is obsolete.

As seen in chapter 4 State of the art – capability and maturity level models and stated in (Salviano & Figueiredo, 2008) the CMMs are not strongly different from each other and are all using a process oriented approach. Therefore every one of the discussed models would be applicable for the use with the ISMS core processes and a formal in depth analysis of the CMMs as well as the development of more detailed criteria are obsolete.

ISO/IEC 15504 has a broad international acceptance and dominance (Salviano & Figueiredo, 2008) as well as it has itself a high level of maturity. As the ISO/IEC 33000 series is intended to replace the ISO/IEC 15504 standard series the capability/maturity model of ISO 33020 (*Information technology -- Process assessment -- Process measurement framework for assessment of process capability*, 2015a) is used in this thesis, which already answers MRQ2-3.

As a result of this considerations only research question MRQ2-2 is left to be analyzed within a SLR and used to verify or dismiss the suitability of ISO 33020 as answer to the research question MRQ2-3.

6.2 SLR – Analysis of the latest research regarding maturity level model use within an ISMS

To answer MRQ2-2 “Are maturity models already used within ISMS?” a systematic literature review (SLR) has been conducted. A systematic review is “a means of evaluating and interpreting all available research relevant to a particular research question, topic area or phenomenon of interest” (Keele, 2007). “Systematic literature reviews in all disciplines allow us to stand on the shoulders of giants and in computing, allow us to get off each other’s feet” (Keele, 2007). On the basis of Kitchenham (2004, p. 2) the reasons for performing this SLR were:

1. To identify if there is a gap in the current research regarding the use of maturity level models within an ISMS
2. To provide background in order to appropriately position new research activities (to develop a method for the use of maturity level models within an ISMS

The SLR was performed using the following steps based on Kitchenham (2004):

1. Planning the review:
   a) Identification of the need for a review
   b) Development of a review protocol
2. Conducting the review
   a) Identification of research
   b) Selection of primary studies
   c) Study quality assessment
   d) Data extraction and monitoring
   e) Data analysis
3. Reporting the review

6.2.1 Planning the review

6.2.1.1 The need for a systematic review

According to Kitchenham (2004) "The need for a systematic review arises from the requirement of researchers to summarize all existing information about some phenomenon in a thorough and unbiased manner." In this case all information regarding the use of maturity level models within an ISMS available in the current research need to be identified to answer MRQ2-2 "Are maturity models already used within ISMS?" as objective of the SLR.

To identify if any existing SLR regarding the use of maturity level models within an ISMS are available the following databases were searched with the search strings ("SLR" AND "ISMS" AND "Maturity"):

- IEEE – 1 result (Delgado & Velthuis, 2014), which is focused on IT governance framework initiatives and not on the usage of maturity level models within an ISMS.
- ACM – 0 results
- Science direct – 38 results – after reading the titles no result was found to cover a SLR regarding the use of maturity level models within an ISMS. All results focus on a different aspect like oceanography, CMMI in software development or maturity level models in ITIL.

As a result no primary study was found regarding use of maturity level models within an ISMS, which arises the need to perform an own SLR. The following restrictions regarding the search for primary studies are present:

- Research string could be to narrow:

  This limitation was dealt with the use of a second search string "SLR" AND "maturity"

- IEEE – 6 results, by reading the title 4 of them were excluded because they do not contain an SLR regarding the usage of maturity level models within an ISMS. The remaining two were:
  - "Development of maturity models: A systematic literature review" (García-Mireles, Moraga, & García, 2012) which is focused in general on maturity level models. Main result of this SLR is, that most of the maturity level models are based on CMM, ISO/IEC 15504 and CMMI-DEV.
  - "An assessment model of information security implementation levels" (Stambul & Razali, 2011) which is focused on measurement parameters. It is specifically designed to answer the research question MRQ2-2.
- ACM – 1 result: "Evidence in software architecture, a systematic literature review" (Qureshi, Usman, & Ikram, 2013), which is focused on software engineering.
- Science direct – 460 results – after reading the titles of the first 52 results as a sample, only two relevant results were found:
  - "Business process maturity models: A systematic literature review" (Tarhan, Turetken, & Reijers, 2016) – a study which covers in general the usage of maturity level models in business process management
  - "An Information Security Maturity Evaluation Mode" (Xiao-yan, Yu-qing, & Li-lei, 2011a) which is also focused on measurement of information security. This is to answer the research question MRQ2-2. Additionally the information provided in this study regarding the SLR and there results are very limited.

  A review of the titles of the remaining results was stopped because the probability of finding any relevant papers was estimated as to low.

Additionally a search with google scholar was performed with the same search strings. As a result "Systematic literature review of software process capability/maturity models," (von Wangenheim et al., 2010) was found. This study is also not focused on the use of maturity level models within an ISMS, but in (von Wangenheim et al., 2010) as a result of a systematic literature review on capability/maturity models it is stated the most models are concentrated around the CMM/CMMI framework and the standard ISO/IEC 15504 (SPICE). This is of interest as it supports the choice of ISO 33020 [73] as answer to MRQ2-3.

To further deal with this limitation a broader search string must be used within the SLR to avoid overlooking any relevant research.

- The searched databases could not be the most relevant databases: According to Kitchenham et al. (2011) and Turner (2010) the searched databases are the most relevant databases. Additionally a search with google scholar and the same search strings was conducted which does not result in the identification of any further relevant research."

As a result even with a more broaden search string, no relevant study could be found which focus on the use of maturity level models within an ISMS, except of some studies focusing on the measurement of information security maturity and not on the general usage of maturity level models within an ISMS.

6.2.1.2 Review protocol

The review protocol is included as Appendix G – Review protocol for the SLR regarding the usage of maturity level models within an ISMS.

6.2.1.3 The research question

According to Kitchenham (2004) "the critical issue in any systematic review is to ask the right question. In this context, the right question is usually one that:

- Is meaningful and important to practitioners as well as researchers.
- Will lead either to changes in current "…" practice or to increased confidence in the value of current practice.
- Identify discrepancies between commonly held beliefs and reality.

Additionally, Kitchenham (2004) states that "a systematic review in a PhD thesis should identify the existing basis for the research student's work and make it clear where the proposed research fits into the current body of knowledge."

The research question MRQ2-2 "Are maturity models already used within ISMS?" will identify the existing basis to answer MRQ2: Are there maturity level models and methods applicable for information security management processes existent? This will result in reaching objective 2 – "Select or modify an existing maturity level model for the use with the ISMS core process framework". A maturity level model for the usage within an ISMS will fit into the existing current body of knowledge as maturity level models are used within other disciplines as software engineering or IT- and service management.

6.2.2 Conducting the review

6.2.2.1 Generating a search strategy

The following strategy was used for the construction of search terms:

A. Use the research question for the derivation of major terms;
B. For these major terms, find the alternative spellings and synonyms;
C. Use of Boolean operators for conjunction in such a way, to use 'OR' operator for the concatenation of alternative spellings and synonyms whereas 'AND' for the concatenation of major terms.

The research question MRQ2-2 consists of two groups of terms:

- Group 1: Information security terms
  - ISMS
  - Information Security Management System
  - Information Security Management
  - Information Security
- Group 2: Maturity level model terms
  - Maturity Level
  - Maturity Level Model
  - Process Maturity

The resulting search string is the following:

"ISMS" OR "Information Security Management System" OR "Information Security Management" OR "Information Security" + "Maturity Level" OR "Maturity Level Model" OR "Process Maturity"

6.2.2.2 Study selection criteria

Regarding the selection of the search strategy respectively the search tools and databases the following factors were taken into account:

For performing the search it is essential, that the search tools or databases offer features for an easy evaluation of the search results like for example showing how often an item has been cited. For efficiency reasons it is important to get fast access and have the possibility to export bibliographic data to Zotero which is used by the author of this thesis as a reference management tool.

Based on Kitchenham et al. (2011) and Turner (2010) the following most relevant databases were searched:

- IEEE
- ACM
- Science direct

To avoid publication bias the search string was also used to scan for relevant literature using google scholar.

The following table contains the search process documentation in detail

#	Name of the database or other source	search string	Date of the search	years covered by the search (see EC1)	number of results
1	IEEE	*(ISMS OR Information Security Management System OR Information Security) AND (Maturity Level OR Maturity Level Model OR Process Maturity)* *search in full text and metadata using advanced search*	April 5rd 2016	January 2015 till April 2016	1789 (after applying EC1: 155)
2	ACM	*("ISMS"; "Information Security Management System"; "Information Security Management"; "Information Security") AND ("maturity level"; "maturity level model"; "process maturity")* *search in the ACM Full Text Collection using advanced search*	April 5rd 2016	January 2015 till April 2016	1 (after applying EC1: 0
3	Science direct	*"ISMS" OR "Information Security Management System" OR "Information Security Management" OR "Information Security" AND "maturity level" OR "maturity level model" OR "Process maturity" AND LIMIT-TO(topics, "system,security,model,risk")* search in all fields using expert search of science direct	April 5rd 2016	January 2015 till April 2016	1089 (after applying EC1: 197)

#	Name of the database or other source	search string	Date of the search	years covered by the search (see EC1)	number of results
4	Google Scholar	*"ISMS" OR "Information Security Management System" OR "Information Security Management" OR "Information Security" AND "maturity level" OR "maturity level model" OR "Process maturity"*	April 5rd 2016	January 2015 till April 2016	ca. 2500 (after applying EC1: 417)

Table 39 – Search process documentation – SLR ISMS processes

6.2.2.3 Performing the selection process

The following selection criteria of the results were defined by the author of this thesis:

- Exclusion criteria – EC1: Exclude any study or paper which is older than January 2015
- Exclusion criteria – EC2: Exclude any study/paper where the title suggests that the paper is not focused on ISMS and maturity level models and the title is not available in English or German.
- Exclusion criteria – EC3: Exclude any study/paper where the abstract shows the paper is not focused on ISMS and maturity level models.
- Inclusion criteria – IC1: Include all studies or papers which does not meet one of the exclusion criteria EC1 to EC3

The search with Google Scholar produced 2.500 hits. After applying EC1 417 hits were left which were analyzed regarding the exclusion criteria EC2 to EC3. After that 214 studies and papers were left.

Searching in IEE, ACM, Science direct and google scholar produced the following results:

- IEEE: 1789 hits, after applying EC1: 155 hits
- ACM: 1 hit, after applying EC1: 0 hits
- Science direct: 1089 hits, after applying EC1: 197 hits
- Google scholar: 2500 hits, after applying EC1: 417 hits

Within the screening of the titles (EC2) all papers or studies were excluded if the title suggests that a different topic than ISMS or ISMS processes is the focus of the paper.

Screening the titles showed that a majority of the identified papers/studies do meet the EC2 as they are dealing mostly with single processes like the awareness process (Poepjes, 2015) or software engineering/development.

It is supposed that the reason for that is the CMM has a very strong history in software engineering and the general advantages of maturity level models within information security management are not recognized yet.

For example the following papers were obviously not focused on the research question and therefore excluded:

- A survey of information security incident handling in the cloud
- Measuring user satisfaction with information security practices
- A Maturity Model for ISO/IEC 20000-1 Based on the TIPA for ITIL Process Capability Assessment Model
- The interdependent effects of solar disinfestation and compost maturity level on soil microbial activity
- Towards an Implementation of an Interoperable Identity Authentication Framework in e-Government: Case of Malawi

After applying EC2 the following results were left:

- IEEE: 155 hits, after applying EC2: 17 hits
- Science direct: 197 hits, after applying EC2: 23 hits
- Google scholar: 417 hits, after applying EC2: 44 hits

After applying the exclusion criteria EC1 and EC2 the remaining results were assessed regarding the exclusion criteria EC3. For the assessment of the inclusion criteria IC1 it is considered critical to assess the abstract of the papers/studies regarding the question does the abstract shows the paper is focused on ISMS and maturity level models?

After the exclusion of irrelevant papers based on title and abstract and the exclusion of doublets, the researcher finally found three papers or studies which meet the inclusion criteria IC1 and should be included in the data extraction and analysis:

- (Mitasiunas, Novickis, & Kalpokas, 2014) Security Process Capability Model Based on ISO/IEC 15504 Conformant Enterprise SPICE
- (Coelho, Fernandes Jr, & Proença Jr, 2014) GAIA-MLIS: A Maturity Model for Information Security
- (Slot, 2015) Towards Rule-based Information Security Maturity

The selection process and the results of that process are shown in Figure 8 – Analysis of maturity models and there use within an ISMS.

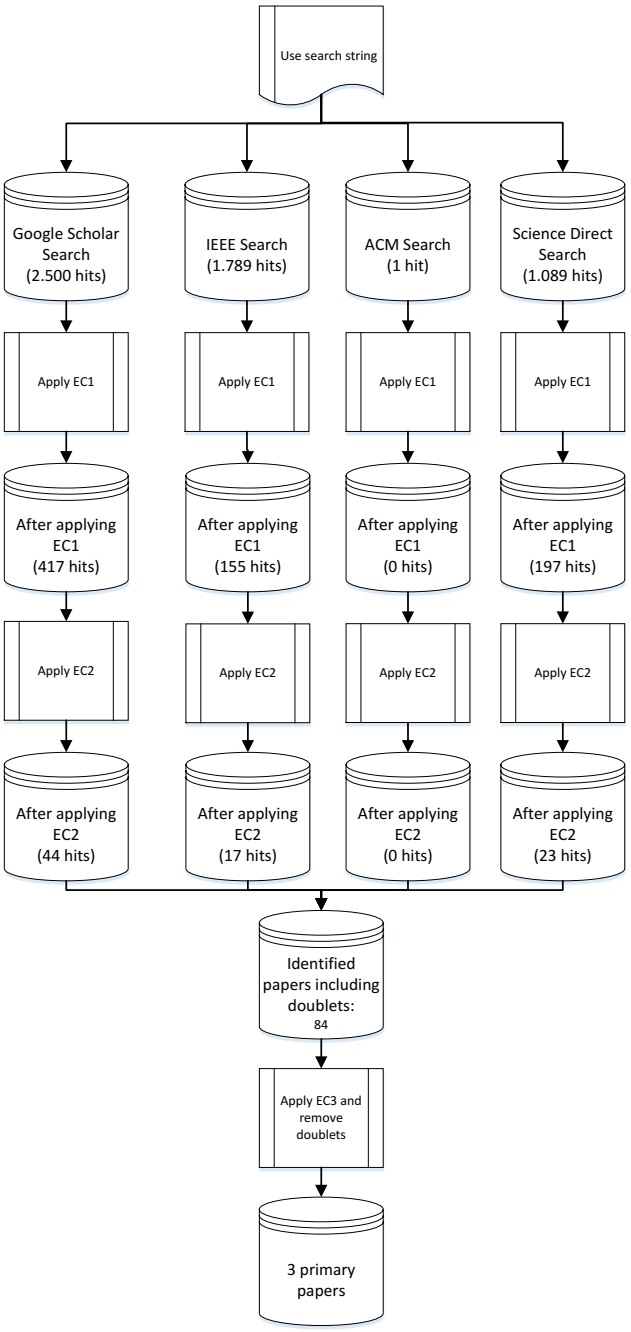

Figure 8 – Analysis of maturity models and there use within an ISMS

6.2.2.4 Study quality assessment

According to Kitchenham (2004) in addition, to general inclusion exclusion criteria, it is generally considered important to assess the "quality" of primary studies but there is no agreed definition of study "quality".

In Mitasiunas et al. (2014) no information is given on which methods the presented solution relies.

As described in (Coelho et al., 2014) the results of this study were verified on a questionnaire with three organizations.

As described in (Slot, 2015) the scientific approach consists of a systematic literature review as well as an expert questionnaire.

Considering this information the quality hierarchy of the identified papers is evaluated as follows (most important is quality hierarchy 1):

#	Paper	SLR	Expert opinion	Case study	Quality hierarchy
1	(Mitasiunas et al., 2014) – Security Process Capability Model Based on ISO/IEC 15504 Conformant Enterprise SPICE	-	-	-	3
2	(Coelho et al., 2014) – GAIA-MLIS: A Maturity Model for Information Security	-	(Questionnaire)	-	2
3	(Slot, 2015) – Towards Rule-based Information Security Maturity	X	X	-	1

Table 40 – Study quality assessment – SLR ISMS maturity level models

6.2.2.5 Data extraction and analysis, limitations and conclusion

In order to answer MRQ2-2: "Are maturity models already used within ISMS?" three primary papers have been identified. Most of the candidates can be described as noise because

- they were not focusing on information security management,
- were focusing on general process management or specific topics actually in the focus of interest like cyber security or cloud security, or
- were not related to the maturity of security management processes.

Nevertheless the main ideas of the identified papers are discussed below.

Mitasiunas et al. (2014) describe security as a critical quality attribute and a process oriented activity. To achieve this, dedicated security-focused processes must be defined and implemented. Given the process-based view of security, related process capability needs to be continuously evaluated and improved according to Mitasiunas et al. (2014).

For this they proposed information security process capability model (ISPCM). “The goal of the development of ISPCM was to build a framework that describes security as a process-oriented activity and is sufficiently detailed as a tool for any organization that wishes to assess and increase the capability of the security quality attribute of its processes in the context of enterprise-wide process improvement” (Mitasiunas et al., 2014). Even security certifications could be based on process capability assessment using the ISPCM according to Mitasiunas et al. (2014).

ISPCM contains a process not mentioned in the ISO 27000 series called “security implementation management”. This process is partially integrated in information security change management process and information security governance process of the proposed ISMS core process framework of this thesis. All other proposed processes were also already integrated in the ISMS process framework. So no new processes needs to be integrated in the ISMS core process framework, but Mitasiunas et al. (2014) also figured out, that capability and maturity models could be of use in ISMSs.

According to Coelho et al. (2014) there is a great demand for a tool which is able to demonstrate the maturity level of an information security system. The proposed GAIA-MILS model is intended to be used to analyze the maturity level of an organization’s information security system and supply them with key data on how they can improve it. Agreeing with Coelho et al. (2014) organizations should assess their level of safety maturity through a formal model and utilize it as a parameter to measure the security risk. For this, the proposed GAIA Maturity Level Information Security (GAIA-MLIS) aims to assess the maturity level of information security observing five areas (hardware, software, staff, facilities and information) through a diagnostic evaluation. But the model does not recognize any ISMS processes. Coelho et al. (2014) also recognizes COBIT as a helper tool for the development of a model of maturity level in information security.

Slot (2015) proposes a rule based information security maturity model, based on a focus area maturity model. A focus area maturity model is a specific type of maturity model. As opposed to the traditional maturity models that have a fixed number of generic maturity levels, the focus area maturity matrix defines maturity levels per aspect or focus area within a functional domain (Slot, 2015; Van Steenbergen, Bos, Brinkkemper, Van De Weerd, & Bekkers, 2010).

According to Slot (2015) “The Information Security Focus Area Maturity (ISFAM) model is an in Excel developed focus area maturity model, which was created in 2013. It consists of four focus area categories (organizational, technical, organizational and technical, and support) which cluster 13 different focus areas, and distribute 51 capabilities (A-E) over 12 maturity levels. The focus areas and capabilities of the ISFAM model were determined by comparing five information security standards: ISO 27K, Information Security Framework (based on ISO), Standard of Good practice (ISF), and IBM security framework, and was evaluated by information security experts.”

ISFAM focus areas have only partially an expression in the proposed core processes of the ISMS core process framework of this thesis. This is depicted in Table 41 – ISFAM focus areas and there representation in the proposed ISMS core process model.

ISFAM focus area	Expression in ISMS core process model
Organizational	
1. Risk Management;	Information security risk assessment and treatment process
2. Policy Development;	No direct expression
3. Organizing Information Security;	ISMS planning process and partially Information security governance process
4. Human Resource Security;	No direct expression
5. Compliance;	Requirements management process
Technical	
6. Identity and Access Management;	No direct expression
7. Secure Software Development;	No direct expression
Organizational and Technical	
8. Incident Management;	Information security incident management process
9. Business Continuity Management;	No direct expression
10. Change Management;	Partially Information security change management process
Support	
11. Physical and Environmental Security;	No direct expression
12. Asset Management;	No direct expression
13. Architecture	No direct expression

Table 41 – ISFAM focus areas and there representation in the proposed ISMS core process model

Therefore the use of the results of (Slot, 2015) in the proposed ISMS core process model is limited.

The following table sum up the results of the analysis of the identified papers:

Paper	Does it contain ISMS processes?	Does it contain a maturity level model	Does it contain evidence or empirical studies about the usage of maturity models within information security management systems
(Mitasiunas et al., 2014) Security Process Capability Model Based on ISO/IEC 15504 Conformant Enterprise SPICE	Yes	Yes	No
(Coelho et al., 2014) GAIA-MLIS: A Maturity Model for Information Security	No	Yes	No
(Slot, 2015) Towards Rule-based Information Security Maturity	Partially	Yes	No

Table 42 – SLR analysis results regarding maturity level model usage within ISMS

So no paper does contain any resilient information about the actual usage of maturity level models within ISMS.

Limitations and second data extraction

EC 1 and the chosen search engines could be a too narrow criteria for this systematic literature review because resigning EC1 and using a Google search with the string "Information security maturity" produced further papers which were additionally analyzed informally and snowballing techniques were used to identify further papers and studies. Guidelines like (B. A. Kitchenham et al., 2011) do not explicitly recommend snowballing and snowballing is not used in most systematic literature reviews as a complement to searching the databases, but according to (Jalali & Wohlin, 2012) it is – if combined with traditional SLR methods – a suitable and efficient method, resulting in proper results while dramatically reducing the amount of noise in database searches.

Identified papers are:

- (Stevanović, 2011) – Maturity Models in Information Security
- (*Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)*, 2008) – System Security Engineering Capability Maturity Model (SSE-CMM)
- (Stacey, 1996) – The Information Security Program Maturity Grid
- (Karokola, Kowalski, & Yngström, 2011) – Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View
- (Phillips, 2003b) – Using a Capability Maturity Model to Derive Security Requirements
- (Saleh, 2011) – Information Security Maturity Model
- (Matrane & Talea, 2014) – Towards A New Maturity Model for Information Security Management
- (Bowen & Kissel, 2007a) – NIST IR 7358 – Program Review for Information Security Management Assistance (PRISMA)
- (Norman & Yasin, 2013) – Information Systems Security Management (ISSM) Maturity Factors In E-Commerce Malaysia
- (The Open Group, 2011) - The Open Group Information Security Management Maturity Model (see chapter 0)
- (Anderson, 2014) - From Here to Maturity - Managing the Information Security Life Cycle
- (Eshlaghy, Pourebrahimi, & Nobari, 2011) - Presenting a Model for Ranking Organizations Based on the Level of the Information Security Maturity
- (Siponen, 2002) - Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria
- (Gottschalk & Solli-Sæther, 2006) - Maturity model for IT outsourcing relationships
- (Xiao-yan, Yu-qing, & Li-lei, 2011b) - An Information Security Maturity Evaluation Mode

- (Sanchez, Villafranca, & Piattini, 2007) - MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs
- (Cholez & Girard, 2014) - Maturity assessment and process improvement for information security management in small and medium enterprises

Ideas and concepts of this papers and studies are discussed briefly in the following:

Looking at information security maturity models for SMEs, (Sanchez et al., 2007) developed a model for SMEs called the Maturity Model for Security Management in SMEs (MMISS-SME). Another information security maturity model for SME is described in (Cholez & Girard, 2014).

According to (Stevanović, 2011) the idea of adding maturity models to some of the information security standards emerged from the fact that the information security is the result of many activities.

Maturity Model or ISM3 (more often – ISM3) represents one of the standards from the information security area, whose main goal, apart from achieving the admissible level of security, is achieving business results. ISM3 is process oriented approach, like ITIL. With maturity model being the integral part of the standard, it is necessary to give management the tool for identifying which benefits ISMS gives to the organization, which processes can be improved and in what extent. ISM3 is focused on measurement of these processes that are under direct control of ISMS (Stevanović, 2011).

System Security Engineering Capability Maturity Model (SSE-CMM) is a standard (ISO 21827:2008 (*Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)*, 2008)) of similar characteristics like ISM3. The first version of SSE-CMM was published in 1994. SSE-CMM describes the basic characteristics that an organization must provide in order to achieve the admissible level of information security. Like ISM3, SSE-CMM is also process oriented, but it`s character is strictly technical and it doesn`t treat business result as a main goal of maturity model (Stevanović, 2011). The SSE-CMM defines eleven security-related process areas:

- PA01 – Administer Security Controls
- PA02 – Assess Impact
- PA03 – Assess Security Risk
- PA04 – Assess Threat
- PA05 – Assess Vulnerability
- PA06 – Build Assurance Argument
- PA07 – Coordinate Security
- PA08 – Monitor Security Posture
- PA09 – Provide Security Input
- PA10 – Specify Security Needs
- PA11 – Verify and Validate Security

In general, (Stacey, 1996) describes five stages of information security maturity: uncertainty, awakening, enlightment, wisdom and benevolence. In each stage five criteria are represented: management understanding and attitude, security organization status, incident handling, security economics, security improvement actions.

In Karokola et al. (2011) a comprehensive information security maturity model (ISMM) that addresses both technical and socio/nontechnical security aspects is proposed. ISMM uses five maturity levels, which were: undefined, defined, managed, controlled and optimized. In (Karokola et al., 2011) a total of eight existing ISMMs were selected, critically analyzed:

- Information security management maturity model (Aceituno, 2007),
- NIST (PRISMA) information security maturity model (Bowen & Kissel, 2007b),
- Generic security maturity model (GSMM) (Lessing, 2008)
- Gartner's information security awareness maturity model (GISMM) (Dzazali, Sulaiman, & Zolait, 2009),
- SUNY's information security initiative (Lessing, 2008),
- IBM information security framework (Buecker, Borrett, Lorenz, & Powers, 2010),
- Citigroup's information security evaluation maturity model (Masinsin & Corps, 2008),
- Continuous learning and improvement framework (CLIF) (Rao & Jamieson, 2003),
- ISMS (Im)–maturity model (Woodhouse, 2008).

The proposed information security maturity model (ISMM) of (Saleh, 2011) relies on four core indicators for benchmarking and as an aid to understanding the security needs in the organization. These four indicators are domain specific rather than being process specific but they measure the aspect of structure, the management, the practices and the overall performance of the of the organization in term of its security.

Matrane & Talea (2014) and Lindström, Samuelsson, Harnesk and Hägerfors (2008) states, that "Information security management standards like ISO 27001, GASPP/GAISP and SSE-CMM which are widely utilized and advocated by researchers and practitioners alike have a limitation in that they focus on ensuring that security processes exist while being unconcerned about how these security processes can be accomplished in practice". In Matrane and Talea (2014) a maturity model of information security management is proposed consisting of distinct phases of information security management: business management, risks management, operations management, incidents management and problems management. For each phase three maturity levels with critical success factors are defined.

The NIST provided with Bowen and Kissel (2007a), an interagency report containing an overview of the NIST Program Review for Information Security Management Assistance (PRISMA) methodology. "PRISMA is a tool developed and implemented by NIST for reviewing the complex information security requirements and posture of a federal information security program" (Bowen & Kissel, 2007a). The structure of PRISMA is based upon the Software Engineering Institute's (SEI) former Capability Maturity Model (CMM). PRISMA consists of nine primary review topic areas of information security (1. Information Security Management and Culture; 2. Information Security Planning; 3. Security Awareness, Training, and Education; 4.Budget and Resources; 5.Life Cycle Management; 6.Certification and Accreditation; 7.Critical Infrastructure Protection; 8. Incident and Emergency Response; 9. Security Controls) and five maturity levels (Maturity Level 1: Policies; Maturity Level 2: Procedures; Maturity Level 3: Implementation; Maturity Level 4: Testing; Maturity Level 5: Integration) which are combined in a matrix to a maturity based scorecard of information security. The topic areas of information security are not process oriented and therefore not compatible with the proposed ISMS core process framework and PRISMA also includes no methodology to determine the necessary maturity of the topic areas. PRISMA is focused on the maturity of an information security program and not on single processes. So a use of PRISMA with the proposed ISMS core process model is not possible.

Norman and Yasin (2013) is a study which aims to investigate and determine ISSM maturity factors and its relationship with the organizational context in the Malaysian SMI/E e-Commerce. They recognized that each business has its unique information systems security management maturity (ISSM) requirements and demands unique implementation in accordance with its business objectives. They also recognized that ISSM maturity requires process adoption diffusion of security management. They found out, that from the studied variables (business age, organization size, e-commerce stage and top management support only the variable e-commerce stage is negatively influencing achieving ISSM maturity. All other variables show no support towards ISSM maturity. But the findings of this study are limited to a specific business context and cannot be generalized. Therefore the findings of this study are not used in this thesis. Anderson (2014) states that it is possible for no correlation to exist between the overall maturity of the organization and its information security program. Also three major factors influencing the maturity of information security are identified, which will be considered in the development of a method to identify the necessary maturity level (see chapter 7):

- Technological change drives information security programs to evolve and mature to meet the challenges created by innovation.
- Regulatory requirements: Without appropriate leadership and executive support, the resulting information security program may remain in an early compliance-centric state.
- Major external security events often fuel increases in maturity because they put security into the spotlight and get the attention of executives.

Anderson (2014) also proposes an adaptation of the Nolan model for information security organizations using a six-step maturity paradigm: Initiation, Contagion, Control, Integration, Data administration and Continuous renewal.

Eshlaghy et al. (2011) propose a model based on the knowledge of multi criteria decision making to rank organizations about the level of the information security maturity. They also found out that no research has been performed till than about ranking organizations based on the level of the information security maturity.

Siponen (2002) recognizes in 2002 that information security maturity criteria have so far received inadequate attention in information security circles. "This is intriguing, given that the maturity ventures are currently the latest stage in the evolution of the checklist-management standard concept" But any information security checklist or management standard can be turned into a maturity criterion simply by dividing the checklist or management standard into maturity levels. In this paper (*Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)*, 2008; Murine & Carpenter, 1984; Stacey, 1996) are identified as maturity approaches for information security management and summarized as depicted in Table 43 – Maturity approaches for information security management.

Name	Key ideas	Sources of influence
SSE-CMM	Five maturity levels	CMM
Information security program maturity grid	Five maturity levels	CMM, the quality management maturity grid
Software security metrics	11 high-level security criteria and five milestones	-

Table 43 – Maturity approaches for information security management

(Siponen, 2002) summarizes six lessons that information security maturity criteria can learn from software engineering literatures and that Information security management standards can be regarded as a legacy of checklists.

Lessons are:

1. **Operational focus** – The point of the operational focus is to ponder whether the information security maturity criteria uphold conventionalism (and have an operational focus), or do these criteria support reforms and innovations).
2. **Naturalistic mechanistic view** - even if the naturalistic-mechanistic view would be adequate for software development, it is definitely not an adequate framework for approaches aimed at securing organizations' information systems.
3. **Stable, non-emergent, organization structures and functions** – Development methods are suited to stable organizations and not for emerging organizations. Any modern information security maturity method should support the requirements posed by emergent organizations. In other words, a successful method should be able to adapt rapidly to ever-changing requirements owing to a fast paced business environment.
4. **Double standard** – The problem of double standard refers to a situation where an organization manipulates its results in order to look better in a maturity evaluation. So there must be ``objective and universal'' criteria, which are able to indicate the maturity of all kinds of organizations.

5. **Spot focus** – Spot focus is the criticism that the focus of maturity inspection is on prefixed spots, the result being that the criteria do not pay any attention to a holistic overall maturity posture.
6. Degree of ambiguity in maturity criteria – refers to the problem of different degree of ambiguity in maturity criteria from "reference only" to "subjective", "partially objective" and "objective".

It is concluded in Siponen (2002), that there are two categories of information security maturity standards:

- General information security management standards (mainly for inter-organizational self-assessment)
- Information security maturity management oriented endeavors (inter-organizational self-assessment and public dimension assessment).

Gottschalk and Solli-Sæther (2006) and Poepjes (2015) are not relevant for an ISMS maturity level model as they focus on the maturity of specific processes of the ISMS (awareness and outsourcing). Nevertheless this is relevant for further research on a process specific level.

Mayer and Fagundes (2009) also focusses on a specific ISMS process and proposes a model to assess the maturity level of the information security risk management process according to ISO 27005. For the information risk management process 35 control objectives were identified and mapped to the maturity levels as shown in Table 44 – Control map to be implemented in each activity per maturity. Also a generic RACI-Chart is provided for the control objectives.

Risk management activities	**Maturity levels** **Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Context definition	no control is implemented	CD1.1,CD1.2,CD1.3	CD1.4,CD1.5,CD1.6,CD1.7	CD1.8	CD1.9
Risk analysis/assessment	no control is implemented	AA1.1,AA1.2	AA1.3,AA1.4,AA1.5	AA1.6	AA1.7,AA1.8
Risk treatment	no control is implemented	RT1.1	RT1.2, RT1.3, RT1.4, RT1.5, RT1.6	RT1.7	RT1.8
Risk acceptance	no control is implemented	RA1.1,RA1.2	RC1.2,RC1.3	RC1.4,RC1.5	RC1.6

Risk management activities	Maturity levels Level 1	Level 2	Level 3	Level 4	Level 5
Risk communication	no control is implemented	RC1.1	MA1.2,MA1.3	MA1.4	MA1.5
Monitoring and critical risk analysis	no control is implemented	MA1.1			

Table 44 – Control map to be implemented in each activity per maturity

This is of interest for further research as it provides a method for identifying process specific control objectives per maturity level.

Xiao-yan et al. (2011b) also performed an SLR on ISMS maturity identifying papers, studies and standards, which were already identified in this thesis. So this paper is not further considered in the later chapters.

The following table sum up the results of the analysis of the within snowballing and google search identified additional papers:

Paper	Does it contain ISMS processes?	Does it contain a maturity level model based on ISO 15504	Does it contain evidence or empirical studies about the usage of maturity models within information security management systems
(Stevanović, 2011) – Maturity Models in Information Security	No	Partially	No
(*Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)*, 2008) – System Security Engineering Capability Maturity Model (SSE-CMM)	Partially	Yes	No
(Stacey, 1996) – The Information Security Program Maturity Grid	Yes	Yes	No
(Karokola et al., 2011) – Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View	Yes	Yes	No

Paper	Does it contain ISMS processes?	Does it contain a maturity level model based on ISO 15504	Does it contain evidence or empirical studies about the usage of maturity models within information security management systems
(Phillips, 2003b) – Using a Capability Maturity Model to Derive Security Requirements	Yes	Yes	No
(Saleh, 2011) – Information Security Maturity Model	Yes	Yes	No
(Matrane & Talea, 2014) – Towards A New Maturity Model for Information Security Management	Yes	Yes	No
(Bowen & Kissel, 2007a) – NIST IR 7358 – Program Review for Information Security Management Assistance (PRISMA)	Partially	Yes	No
(Norman & Yasin, 2013) – Information Systems Security Management (ISSM) Maturity Factors In E-Commerce Malaysia	No	No	Partially
(The Open Group, 2011) - The Open Group Information Security Management Maturity Model (see chapter 0)	Yes	Yes	No
(Anderson, 2014) - From Here to Maturity - Managing the Information Security Life Cycle	No	Yes	No
(Eshlaghy et al., 2011) - Presenting a Model for Ranking Organizations Based on the Level of the Information Security Maturity	No	Partially	No
(Siponen, 2002) - Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria	No	No	No
(Gottschalk & Solli-Sæther, 2006) - Maturity model for IT outsourcing relationships	Partially	Partially	No
(Xiao-yan et al., 2011b) - An Information Security Maturity Evaluation Mode	No	No	No

Paper	Does it contain ISMS processes?	Does it contain a maturity level model based on ISO 15504	Does it contain evidence or empirical studies about the usage of maturity models within information security management systems
(Sanchez et al., 2007) - MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs	Yes	Yes	No
(Cholez & Girard, 2014) - Maturity assessment and process improvement for information security management in small and medium enterprises	Yes	Yes	No

Table 45 – SLR analysis results regarding maturity level model usage within ISMS

As a result of the data extraction, no paper does contain any resilient information about the actual usage of maturity level models within ISMS. Most papers try do define their own approach how to measure maturity. Some papers are focusing on individual processes where other papers are investigation what factors are influencing the ISMS maturity.

Conclusion

As seen in the data extraction and analysis as well as the limitations part maturity models are used within ISMSs and there are a limited number of research papers or studies in this field. But (Matrane & Talea, 2014) also identifies a lack of researches in the field of Information Security Management and maturity models.

As a result of this analysis it seems that maturity level models are used within an ISMS, but no resilient information about the actual usage of maturity level models within ISMS are available. This should be investigated in further research. Methods for applying maturity level models to ISMS processes are actually not in the focus of the actual research and should be further investigated. Ideas and concepts from the papers and studies found using a Google search with the string “Information security maturity” and with snowballing techniques were included in the proposed ISMS core process framework and the method to determine the necessary maturity level of ISMS core processes were suitable.

It is also concluded that the selection of CMMI identical with ISO 15504 as maturity model for ISMS core processes is appropriate because nearly all identified literature are referencing to that models (see Table 45 – SLR analysis results regarding maturity level model usage within ISMS) while not adding or modifying it significantly for the use within ISMS core processes.

7 Method to determine the necessary maturity level

7.1 Approach and development of the method

A systematic literature review (SLR) / mapping study (Kitchenham et al., 2011) was planned to identify and categorize all relevant research papers related to methods for the determination of the necessary maturity level of processes or in particular ISMS core processes to answer the main research question MRQ3-1. The following research question should be answered by the SLR:

- MRQ3-1: What methods are used for the determination of the necessary maturity level?

As already seen in the systematic literature review (SLR) / mapping study (Kitchenham et al., 2011) to identify and categorize all relevant research papers related to capability maturity models and their use in ISMS, no papers or studies were found containing specific information about a method to determine the necessary maturity level model.

Therefore to answer MRQ3-2 "Which method is most suitable to determine the necessary maturity level of ISMS processes?" a new method need to be developed. For this the results from chapter 6 and an informal literature analysis be used to develop a new method for the determination of the necessary maturity level of ISMS core processes:

Mijnhardt, Baars and Spruit (2016) identified organizational characteristics influencing the maturity of information security of an organization but not any detailed method how to use the characteristics to determine a specific process maturity level. The characteristics influencing information security are depicted in Table 46 – Organizational characteristics influencing information security.

General	Outsourcing	IT Dependency	IT Complexity
Number of Employees	Percentage of outsourced vs. insourced software development	Importance of critical data number of employees	Importance of critical data number of employees
Revenue	Percentage of outsourced vs. insourced software hosting / IT services	Importance of confidentiality of critical data	Annual expenditure on IT over revenues
Industry sector		Importance of availability of critical data	
		Possible time without IT Support	

Table 46 – Organizational characteristics influencing information security

Additionally (Saleh, 2011) identified four domains that affect security at the organization: organization governance, organizational culture, the architecture of the systems and service management.

As a result an additional formal SLR is obsolete from the viewpoint of the author of this thesis, because no additional information is supposed to be found by a further SLR.

According to COBIT 5 for Information Security (Information Systems Audit and Control Association, n.d.-c, p. 87,88) the target capability for information security shall be defined individually by every organization. In addition, the target maturity levels would be expected to vary for different individual IT processes, IT infrastructures and industry characteristics (Information Systems Audit and Control Association, 2008, p. 18).

The available information security standards underline the differences of information security per industry sector. Sector specific standards for information security are for example:

- ISO 27799: Health informatics - Information security management in health;
- ISO/IEC TR 27015: Information technology - Security techniques - Information security management guidelines for financial services;
- ISO 27011: Security techniques - Information security management for telecommunications;
- ISO 27019: Security techniques - Information security management based on ISO27K for process control systems specific to the energy industry.

Every organization needs to define and implement its own information security enablers depending on factors in the organization's specific internal and external environment. One of these factors is the maturity level of the information security processes (Information Systems Audit and Control Association, n.d.-c, p. 55).

ISACA (Information Systems Audit and Control Association, 2008, p. 8) states that organizations can determine what their target levels should be only by performing a self-assessment balanced with a careful risk assessment.

Attributes of process maturity according to (Information Systems Audit and Control Association, 2008, p. 8) are:

- Awareness and communication – Awareness
- Policies, standards and procedures – Policies
- Tools and automation – Technology
- Skills and expertise – Skills
- Responsibility and accountability – Responsibility
- Goal setting and measurement – Goals

The ISMS core processes differ in terms of volume of their outputs, variety of their outputs, variation in demand of their outputs and the degree of visibility they have (Slack et al., 2010).

In general the adequate maturity level is defined by a management decision based on:

- Risks – what are the risks to operate the process at a specific level?
- Benefits – what are the benefits to a specific level?
- Costs – what does it cost to operate the process at a specific level?
- Maturity level of core business processes

According to an ISACA study (Information Systems Audit and Control Association, 2008, p. 65) the general process maturity differs between organizations in emerging countries (average process maturity level of 2,2) and organizations in developed countries (average process maturity level of 2,9). Also the size of IT operations influences the general process maturity: None of the means of the process maturity for the smaller enterprises broke above 3.0, whereas most of the means of the process maturity were 3.0 or higher for larger enterprises (Information Systems Audit and Control Association, 2008, p. 66).

Finding the adequate maturity level for ISMS core processes also means discussing performance objectives of those processes. Regarding (Slack et al., 2010) performance objectives of processes in general are:

- Quality – doing the right things – consistently producing services or products as specified,
- Speed – doing things fast – is often an important aspect of customer satisfaction,
- Dependability – doing things in time – for customers to receive their products or services exactly when they are needed,
- Flexibility – changing what they do – adapt to changing circumstances quickly without disrupting the rest of the operation,
- Costs – doing things cheaply – efficient use of resources – doing only the necessary things with minimal costs.

The question is which level of those performance objectives need to be met for the individual ISMS core processes. To answer this question it needs to be analyzed how the performance objectives relate to the organizations objectives and vision. COBIT contains mappings which allow to bridge general objectives into IT process objectives (Steiner, n.d.). In general the objectives are (Slack et al., 2010):

- Reducing the costs and reducing the amount of investment
- Achieving customer satisfaction
- Reducing the risk of operational failure
- Providing the basis for future innovation

Practically used objectives are often complement, competing, antinomy or indifferent/neutral and therefore need to be transformed into a well-balanced and harmonic system of objectives (Steiner, n.d.). This is a precondition for the assessment of necessary maturity levels of ISMS processes.

Some authors say, ISO 27001 certified organizations may seek to be recognized as that SSE-CMM Level 5 organization (Saint-Germain & others, 2005). But at an intuitive level, organizations cannot justify the costs of pushing every process to SSE-CMM Level 5 (Information Systems Audit and Control Association, 2008, p. 17). Maturity levels were generic and universal in scope. Consequently they also do not pay enough attention to the differences between organizations and the fact that their security requirements are different (Siponen, 2006b).

7.2 Method proposal

Based on this preliminary considerations the following questionnaire was initially developed by the author of this thesis to identify the necessary maturity level of ISMS processes.

Criteria	Questions	comments
Questions regarding the organization – to be answered only once for an organization		
Organizations objectives and vision	What are the objectives and the vision of the organization?	This is necessary to later analyze how the performance objectives relate to the organizations objectives and vision.
Industry classification	What is the industry classification of the organization? For example: • Capital-intensive industries, other than utilities (Cap) • Utilities (Util) • Service industries (Srv) • Financial institutions (Fin) • Government and non-profits (Govt)	An ISACA study found that the industry classification statistically influences the maturity of the processes (Information Systems Audit and Control Association, 2008, p. 66).
Size of IT operations	What is the size of IT operations taking into account: • IT staff members • Application systems • Clients?	An ISACA study found that the size of the IT operations generally influences the maturity of the processes (Information Systems Audit and Control Association, 2008, p. 66).
Maturity level of core business processes	What is the maturity level of the core business processes?	Mature business processes could be an indicator for the general demand of mature processes (also depending on the size, business model, sector, location). The maturity of the information security program is influenced by the maturity of the organization which is linked to the degree systemic thinking is used in the organization. Systemic thinking paves the way for systemic processes. (Information Systems Audit and Control Association, 2009, pp. 10, 11)

Criteria	Questions	comments
General process specific questions		
Current maturity level of the process	What is the current maturity level of the process?	This is necessary as starting point to analyze later if it is possible to increase or decrease the process maturity.
Complexity of the process	How complex is the process? How many decisions and alternative paths does the process contain?	Complex process flows with multiple alternative paths generally require a higher process maturity (at least level 3) to ensure reliability of process results and to reach process objectives.
Degree of visibility of the process and/or process results	How visible is the process and the process results to - Stakeholders of the process? - the public?	A high visibility of the process or even more of the process results often results in the need for a higher process maturity.
Questions regarding process performance objectives		
Importance of process result quality	How important is the quality of the process results?	The higher the demanded quality of process results, the higher the maturity of the process should be.
Importance of processing speed	How important is a processing time?	If speed is the primary goal of the process, processing time needs to be measured continually. This could be an indicator of maturity level 4 or even level 5.
Importance of process flexibility	How necessary is it to ensure a flexibility of process steps? What degree of flexibility is needed?	If flexibility is the primary goal of the process it seems not sufficient to define every alternative path of the process. So this would be an indicator for maximum maturity level 2.
Importance of process costs	How important is it to ensure minimum costs of process operation?	Minimum costs could be an indicator for a low process maturity as process overhead costs will rise with a higher process maturity. But this is also dependent on the necessary quality of process results. Where a high process result quality is required it could be necessary to rise the process maturity to avoid costs resulting from poor quality of process results.
Dependability	How does the performance objectives of the process relate to the organizations objectives and vision? Which objectives and vision are influenced by the process and/or process results?	The more depended the objectives of the organization (and the more important the objectives are) are form the process or process output the higher the maturity of the process should be.
Questions regarding process output and costs		

Criteria	Questions	comments
Variation in demand of the process outputs	Are there specific points in time were process outputs are critical for other processes and/or for reaching organizations objectives and vision?	If there is a great variation in the demand of the process output this could be an indicator that the process is not often performed. So the staff is usually not trained to perform the process. This could be an indicator for the demand of maturity level 3.
Volume of the process output	What is the volume of the process output?	Processes with a high volume of process output are often performed at a high frequency which means that the staff is usually trained to operate the process (indicator, that level 2 would be sufficient) but could also be an indicator for the demand of a higher maturity level – depending on the dependability of the organization from the process results.
Variety of the process output	How many different process outputs do exist? How great is the variety of the process output?	A great variety of a process output could be an indicator of a complex process with multiple alternative paths. Complex process flows with multiple alternative paths generally require a higher process maturity (at least level 3) to ensure reliability of process results and to reach process objectives.
Costs	How much in terms of money, and work time does one process execution cost?	The higher the cost of the process execution the more it is likely that a high process maturity is required. This is the case because the higher the process costs the more reliability of the process is needed.
Frequency of process operation	How often is the process operated?	A high frequency means that the staff is usually trained to operate the process (indicator, that level 2 would be sufficient) but could also be an indicator for the demand of a higher maturity level – depending on the dependability of the organization from the process results.
Consequences of changing current maturity level		
Costs / Benefits of specific maturity levels of the process	What are the costs to increase the maturity level (for each maturity level left)?	This information is necessary to evaluate if a higher or lesser maturity level of the process could be appropriate.
Costs / Benefits of specific maturity levels of the process	What are the benefits to increase the maturity level (for each maturity level left)?	This information is necessary to evaluate if a higher or lesser maturity level of the process could be appropriate.

Criteria	Questions	comments
Costs / Benefits of specific maturity levels of the process	What are the costs to decrease the maturity level (for each maturity level left)?	This information is necessary to evaluate if a higher or lesser maturity level of the process could be appropriate.
Costs / Benefits of specific maturity levels of the process	What are the benefits to decrease the maturity level (for each maturity level left)?	This information is necessary to evaluate if a higher or lesser maturity level of the process could be appropriate.
Risks	What are the risks to operate the process at specific levels?	This information is necessary to evaluate if a higher or lesser maturity level of the process could be appropriate.
Already communicated or identified requirements regarding the process (dependent also from the industry classification of the organization)		
Legal requirements	Are there specific legal requirements regarding the process or the process results (for example records of the process)?	Already communicated or identified requirements regarding the process are strong indicators for the necessary process maturity.
Customer requirements	Are there requirements of customers to operate the process at a specific maturity level? If so: Which maturity level is stipulated by the customers?	Already communicated or identified requirements regarding the process are strong indicators for the necessary process maturity.
Management requirements	Are there requirements of the management to operate the process at a specific maturity level? If so: Which maturity level is stipulated by the management?	Already communicated or identified requirements regarding the process are strong indicators for the necessary process maturity.

Table 47 – Process maturity criteria

The following table contains the process maturity indicators sorted by the maturity levels.

#	Criteria	Criteria is an indicator for which maturity level?
1	Industry classification	An ISACA study found that the industry classification statistically influences the maturity of some processes (Information Systems Audit and Control Association, 2008, p. 66). Industry classification of the study were: • Capital-intensive industries, other than utilities (Cap) • Utilities (Util) • Service industries (Srv) • Financial institutions (Fin) • Government and non-profits (Govt) The average maturity of the Cobit 4 process ME3 – ensure compliance with external requirements (represented in the ISMS process framework by the process "Requirements management") was: • Cap: 1,5 • Util: 2,0 • Srv: 2,4

#	Criteria	Criteria is an indicator for which maturity level?
		• Fin: 2,8 • Govt: 1,9 The average maturity of the Cobit 4 process ME4 – provide IT governance (represented in the ISMS process framework by the process "Information security governance") was: • Cap: 1,4 • Util: 2,5 • Srv: 2,2 • Fin: 2,6 • Govt: 2,3
2	Importance of process flexibility	Indicator for maturity level 2 or lower
3	Size of IT operations	Indicator for maturity level 2 for small size of IT operations and maturity level 3 or above for high size of IT operations.
4	Costs	For high process operation costs: indicator for maturity level 3 or higher. For low process operation costs: indicator for maturity level 3 or lower
5	Frequency of process operation	For a process with a high frequency of process operation and a high dependability of the organization from the process or process results: indicator for maturity level 3 or higher. In all other cases: indicator for maturity level 2
6	Dependability	For a process with a high dependability of the organization from the process or process results: indicator for maturity level 3 or higher. In all other cases: indicator for maturity level 2
7	Maturity level of core business processes	Indicator for maturity level 3 or higher.
8	Degree of visibility of the process and/or process results	Indicator for maturity level 3 or higher.
9	Importance of process result quality	Indicator for maturity level 3 or higher.
10	Volume of the process output	For a process with a high dependability of the organization from the process or process results: indicator for maturity level 3 or higher. In all other cases: indicator for maturity level 2
11	Variety of the process output	Indicator for maturity level 3 or higher.
12	Variation in demand of the process outputs	Indicator for maturity level 3.
13	Importance of processing speed	Indicator for maturity level 4 or higher.
14	Costs / Benefits of reducing the maturity levels of the process by one level	Depending on the answer: indicator for maturity level 1 to 5
15	Costs / Benefits of reducing the maturity levels of the process by two levels	Depending on the answer: indicator for maturity level 1 to 5
16	Costs / Benefits of increasing the maturity levels of the process by one level	Depending on the answer: indicator for maturity level 1 to 5
17	Costs / Benefits of	Depending on the answer: indicator for maturity level 1 to 5

#	Criteria	Criteria is an indicator for which maturity level?
	increasing the maturity levels of the process by two levels	
18	Legal requirements	Depending on the answer: indicator for maturity level 1 to 5
19	Customer requirements	Depending on the answer: indicator for maturity level 1 to 5
20	Management requirements	Depending on the answer: indicator for maturity level 1 to 5
21	Importance of process costs	Depending on the answer: indicator for maturity level 1 to 5

Table 48 – Indicators sorted by process maturity level

While analyzing the results of the questionnaire to derive the necessary maturity level of the processes the following should be considered:

1) The maturity of processes can be very low (below 1 - Initial), even in large, mature enterprises (Information Systems Audit and Control Association, 2008, p. 9).
2) A study from the ISACA showed that a tight coupling between IT/ISMS processes and processes outside of IT/ISMS result in a relatively high maturity of those processes (Information Systems Audit and Control Association, 2008, p. 9).
3) Generally it should be recognized that answering the questions above will not lead to a computed necessary maturity level. The questionnaire should be used to think about and identify all relevant influencing factors of the necessary maturity level. With this information an informed decision regarding the necessary maturity level of the process should be documented by the management.

To answer questions about the actual maturity of the processes and to develop a plan to bridge the gap between the actual process maturity and the necessary process maturity the maturity of all ISMS processes need to be assessed. For this the in (Information Systems Audit and Control Association, 2008, p. 71) included method can be used analogous:

1) Create a spreadsheet that lists all ISMS processes as rows and the six maturity attributes (Awareness, Policies, Technology, Skills, Responsibility, Goals)
2) Identify process owners and schedule interviews with them (about an hour for each process)
3) Interview (provide maturity attributes (Information Systems Audit and Control Association, 2008, p. 76), take one process at a time, introduce the process, and ask for every maturity attribute of the process.

Another method to assess the actual process maturity is the detailed and complex process assessment model of CobiT (Information Systems Audit and Control Association, n.d.-d).

Part IV – Verification and Evaluation

8 Verification and Evaluation

In this chapter the results of the research are verified and evaluated to identify if they solve the research problem as defined and described in chapter 1 Introduction.

For this the verification and evaluation approach, design and methodologies are described in chapter 8.1 Verification and evaluation approach. In this chapter also a justification of the verification and evaluation methodology and the research methods are presented. Finally, a set of limitations on validity are presented and justified within this chapter.

The following chapters 0 to 8.5 contain the description of verification and evaluation itself.

8.1 Verification and evaluation approach

Solving the problem of the missing standardized process framework for information security management and a method to determine the necessary maturity level of ISMS processes to avoid unnecessary costs requires a set of steps and elements that must be followed in order to build a solution to the problem useful and generalizable.

Since the purpose of this thesis is the definition of a standardized process framework for information security management and a method to determine the necessary maturity level of ISMS processes this requires a verification and evaluation beside the development of the framework and the model.

So, once the first version of the model and the framework is defined, the second phase is the verification and evaluation of the framework and the method.

Phase 1 – Expert study and consultation

For this in a first phase an expert study and an expert consultation will be conducted to collect the opinion of several experts in the field. The aim is to evaluate the overall validity of the elements of the framework and the method to determine the necessary maturity level of the processes of the framework and to gain feedback from experts towards an eventual improvement. This will provide the opportunity to modify, adapt and improve the design of the framework and the method to determine the necessary process maturity levels.

Experts' judgements have been widely used in the information systems arena (Asma'Mokhtar, Yusof, Ahmad, & Jambari, 2016; Chang, 2005; Kautz, Madsen, & Nørbjerg, 2007; Pare, Cameron, Poba-Nzaou, & Templier, 2013; Saeed & Abdinnour, 2013; Worrell, Di Gangi, & Bush, 2013). Shanteau (1992) describes an expert as an individual who has been recognized within his or her profession as having the necessary skills and abilities to perform at the highest level.

This phase consists of two parts:

Part 1 – Verification of the elements of the framework within an expert study. This is described in chapter 0.

Part 2 – Verification of the method to determine the necessary maturity level for ISMS-processes within an expert consultation. This is described in chapter 8.3

Phase 2 – Improvement

The second phase is the improvement of the framework and the method taking into account the results from the expert study and consultation. This is described in chapter 8.4.

Phase 3 – Case study

The last phase is the pilot implementation of the framework in a case study.

A case study research is the most common qualitative method used in information systems (Dubé & Paré, 2003; Myers & others, 1997).

According to (Oates, 2005) a case study is a multi-dimensional tool that is frequently used for seeking answers to specific research inquiries and does not require a researcher to have ability to control over the events and situation like action research does.

Considering this, beside expert consultation and expert study, a case study will be used as the main tool for the verification of the framework and the method to determine the necessary maturity level for ISMS processes.

The objective of the case study is to verify that the framework proposed in this Ph.D. thesis improves management of information security. More specific this case study is aimed to demonstrate the ability of the framework to be implemented and operated while achieving transparency, cost efficiency and ease of use. To evaluate the transparency, cost efficiency and ease of use interviews at every project stage are used. The use of statistical methods to compare the results regarding the cost efficiency before and after implementing the framework is generally not possible. Information necessary for this are not present and cannot be collected quantitatively with a justifiable effort at a reliable level because costs of running an ISMS and costs for the implementation of measures are not divided.

The case study is described in chapter 0.

Limitations on validity

The purpose of this section is to identify and analyze threats of validity. Taking into account that the construction of the framework and the method to determine the necessary maturity level of ISMS core processes was performed using qualitative methods, qualitative methods should be performed for the verification and evaluation.

Validity, in the context of a qualitative study, is defined as the extent to which data are plausible, credible, and trustworthy, and thus can be defended when challenged (Venkatesh, Brown, & Bala, 2013). Agreeing with Lincoln, Lynham and Guba (2011), different types of validity will be considered within this thesis:

1) credibility,
2) transferability and
3) confirmability.

From the viewpoint of **credibility** it must be ensured that the results are believable from the perspective of the participants in the research. Researchers consider that the variety of experts involved in the expert consultation and expert study as well as the interview partners within the case study were enough to reduce their influence in results. Additionally, it is possible to suppose that all experts had comparable levels of knowledge and experience. Given that respondents were in all cases chosen because of their expertise and experience, authors made sure that experts possessed a comparable level of knowledge and expertise.

Transferability is related to the generalizability of research findings. Regarding this two possible threats are identified. The first is the limited number of case studies (one case study was conducted). Although this threat exists, making difficult the generalization of results, it is also true that the case study is representative enough to describe the applicability of the framework. The second threat is, that the participant in the case study was not taken randomly (because of the lack of participants willing to implement the ISMS by using the proposed methodology). It is assumed that generalization of the results is not guaranteed. But the framework as well as the method to determine the necessary maturity level of ISMS core processes and the context and working conditions are not uncommon. So similar implementations are possible for replication.

Confirmability is the degree to which the results could be confirmed or corroborated by others. According to Wester (2011), there are several factors that can influence confirmability results including the thoroughness of one's field notes, summaries, and theoretical notes, which provide an "audit trail" and the transparent nature of the biases of the researchers.

To avoid this bias, an auditor was assigned to the process to assure the quality of the case study, of the expert consultation and of the expert study.

The objective here is to analyze the different threats to the verification and evaluation regarding

- content validity,
- conclusion validity,
- internal validity,
- construct validity and
- external validity.

Content validity is the degree to which items in an instrument reflect the content universe to which the instrument will be generalized (Boudreau, Gefen, & Straub, 2001). This aspect was verified by checking the meaning of the questions in the expert study and expert consultation by sending them to an independent expert, who was not part of the expert study or expert consultation to assess it. This resulted in minor changes regarding the wording of questions.

Conclusion validity is concerned with the relationships between dependent and independent variables, that is, the provision of statistically-correct conclusions based on correct measures and appropriate statistical analyses. In the case of experts study and consultation, it was supposed by the author of this thesis and confirmed by the independent expert, that the sample and its size were convenient and significant enough to test the proposed research questions.

The internal validity is concerned with factors that may affect dependent and which are out of researchers' control. In this case, the author of this thesis believe that this threat should come from the fact that subjects may not have comparable levels of knowledge or expertise. Given that respondents were in all cases chosen because of their expertise and experience, the authors assume that the participants of the expert study and expert consultation have a comparable level of knowledge and expertise because of their roles and partially (if known) their work experience. No significant differences were found, suggesting that the type of respondent and organization did not cause any biases.

Construct validity is the extent to which a construct measures the concepts that it purports to measure (Straub, 1989). It presents two different components: convergent and discriminant validity. Convergent validity assesses consistency across multiple constructs, while discriminant validity examines whether different constructs diverge from one another. Furthermore, construct reliability measures the degree to which measures are free from random error, and therefore yield consistent results. As mentioned earlier an independent expert attended the expert study and expert consultation and also reviewed the approach and the results of the case study to ensure construct validity and reliability.

External validity refers to the extent to which research findings can be generalized, and to what extent the findings are of interest to other purposes. Regarding external validity, two different threats are identified. The first is the size of the sample, which can complicate the generalization of the results. The second is the fact that the sample was not taken randomly.

8.2 Verification of the elements of the framework

To verify or dismiss the identified ISMS core processes or add missing ISMS core processes the author of this thesis conducted a study. In this chapter the method, sample and the results of this study are described and discussed.

8.2.1 Method

As the method to review the identified processes and to verify if the identified ISMS core processes are the most relevant, correct and complete an expert consultation was chosen. In this expert consultation 90 experts were asked to name ISMS core processes in form of a questionnaire. Given was a differentiation in core, management and support processes as well as a list of possible ISMS core processes (as shown in Table 49 – Results of the study to identify ISMS core processes) and the opportunity to name additional processes.

8.2.2 Sample

A panel of 90 German experts in the field of information security was selected, from which 75 experts answered the questionnaire. Roles of the experts were: 53 Information security officers/managers (23 working for private companies; 30 working for public administration), 8 consultants for information security (8 working for private companies) and 14 auditors for information security (3 working for public administration; 11 working for private companies).

8.2.3 Results

The results of this study are documented in Table 49 – Results of the study to identify ISMS core processes and in detail in Appendix D – Results of the ISMS core process study.

Named process (sorted by percentage of naming)	How often was the process named?
ISMS planning process	0 (0%)
Information security risk assessment process	75 (100%)
Information security risk treatment process	74 (99%)
Resource management process	35 (47%)
Process to assure necessary awareness and competence	75 (100%)
Communication process	31 (41%)
Documentation control process	54 (72%)
Requirements management process	30 (40%)
Information security change management process	65 (87%)
Process to control outsourced processes	75 (100%)
Performance evaluation process	66 (88%)
Internal audit process	75 (100%)
Information security improvement process	74 (99%)
Information security governance process	18 (24%)
Information security incident management process	75 (100%)
Service level management process	0 (0%)
Service reporting process	0 (0%)
Service continuity and availability management process	30 (40%)
Budgeting and accounting for services process	4 (5%)

Named process (sorted by percentage of naming)	How often was the process named?
Capacity management process	6 (8%)
Business relationship management process	0 (0%)
Supplier management process	0 (0%)
Incident and service request management process	0 (0%)
Problem management process	3 (4%)
Configuration management process	12 (16%)
Change management process	0 (0%)
Release and deployment management process	0 (0%)
Information security customer relationship management process	71 (95%)

Table 49 – Results of the study to identify ISMS core processes

8.2.4 Discussion of the results from the expert consultation

The results of the expert consultation could be biased because a predefined set of processes was given in the questionnaire. But every expert had the possibility to name additional processes:

- one expert used to name the configuration management process which was also a given process.
- 3 experts named processes regarding the implementation of measures: “security implementation process”, “measurement implementation process”, “control implementation”

Furthermore some processes were integrated in the questionnaire, which were not identified as ISMS core processes in this thesis. So the bias is tolerable.

For the discussion of the results of the study to identify ISMS core processes three categories are defined:

1) Processes which were clearly identified as ISMS core processes – This are processes which were identified by 80% or more of the experts
2) Processes which were not clearly identified as ISMS core processes – This are processes which were identified by not less than 20% but not more than 80% of the experts
3) Processes which were clearly identified as to be not an ISMS core process – This are processes which were identified by less than 20% of the experts.

As seen in Table 49 – Results of the study to identify ISMS core processes, processes which were named as ISMS core processes by a majority of the experts are:

- Information security risk assessment process (100%)
- Process to assure necessary awareness and competence (100%)
- Process to control outsourced processes (100%)
- Internal audit process (100%)
- Information security incident management process (100%)
- Information security risk treatment process (99%)
- Information security improvement process (99%)
- Information security customer relationship management process (95%)
- Performance evaluation process (88%)
- Information security change management process (87%)

All of those processes were also identified as ISMS core processes in this thesis. So as a result of the study this processes were confirmed to be ISMS core processes. It is especially interesting that the process "Information security customer relationship management process" were identified by the experts while this process is not especially named in the ISO 27000 series. This shows that the majority of experts recognized that the management of the relationship to customers of information security is important to maintain an appropriate customer perception and show benefits and value delivered for the invested resources.

As seen in Table 49 – Results of the study to identify ISMS core processes, processes which were not clearly identified as ISMS core processes are:

- Documentation control process (72%)
- Resource management process (47%)
- Communication process (41%)
- Requirements management process (40%)
- Service continuity and availability management process (40%)
- Information security governance process (24%)

Discussion of every process:

The documentation and records control process were identified as an ISMS core process in chapter 5 ISMS core process framework. The study showed that a majority of experts also identified this process as an ISMS core process, but 28% also said that this is not an ISMS core process. This may result from a not clear differentiation of requirement documents like policies and standards on one side and records on the other side. The control of records seems more supportive than a core competency of the ISMS while the control of requirement documents is a core competency of the ISMS. This will be considered in the optimization of the ISMS core process framework by splitting the documentation and records control process is two processes: "Security policy management process" and "Records control process".

Another process identified as an ISMS core process in chapter 5 ISMS core process framework is the “Resource management process”. This process was only identified as an ISMS core process by 47% of the asked experts. This shows a lack of recognition that ISMS resources need to be managed. This is also underlined by the results for the process “Budgeting and accounting for services process”, which only 5% of the experts identified as ISMS core process. This is surprising, because it is commonly recognized in the managements system for IT services that services must be paid and resources need to be managed (International Organization for Standardization and International Electrotechnical Commission, 2011, 2012b) as well as resources management is established in the information security management (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 5). So the idea that services are not available at no costs and costs for information security can and should be charged to the demanding business units where they are no general expenses is not recognized by all ISMS experts. This insight still needs to be learned in the ISMS community. Considering that this process is not identified by the majority of ISMS experts as an ISMS core process and considering that this process is clearly a part of the ISO 27001 the resource manage the author of this thesis still recognizes this process as an ISMS core process. Similarly surprising is that a majority of ISMS experts did not recognize the communication process as an ISMS core process. This may be caused by a lack of awareness for the necessity of a regular and defined communication to stakeholders and customers of the ISMS. But this is not supported by the results for the “Information security customer relationship management process“. Additionally the “Information security governance process” was identified by 24% of the asked experts, which is recognized not as a lack of attention and importance of this process, but as of identifying this process as a management process (also discussed later in this chapter). So it is assumed that the “communication process” is not identified as an ISMS core process because the experts did not understand what is meant with this process in addition to the “Information security customer relationship management process“ and the “Information security governance process”. So the author of this thesis keeps this process as part of the ISMS core processes although this is not clearly confirmed by the asked ISMS experts.

The requirements management process was identified by only 40% of the asked experts as an ISMS core process. This is also surprising, because it can only be explained by a lack of awareness of the experts that identifying the information security requirements is a key success factor of the ISMS. Not knowing the requirements will always result in an inefficient and ineffective ISMS and a not appropriate information security level. Maybe this is, beside the results for the resource management process and the communication management process, also a main reason while information security is still often recognized as cost driver with an intransparent value. Considering the result that this process was also not clearly confirmed in the study as an ISMS core process the author of this thesis also keeps this process as a part of the ISMS core processes because it is clearly identified in (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 7).

The service continuity and availability management process was also identified (40%) by only 40% of the asked experts as an ISMS core process. This was foreseeable, because it is assumed that the process is recognized as part of the IT service management system. The high percentage of experts identifying this process as an ISMS core process was probably resulting from the fact that availability is, beside integrity and confidentiality, one objective of information security. The other 60% seems to recognize the management of availability and continuity as a task of the IT service management system or the business continuity management system while the ISMS is of course interlinked with this managements systems. So, although it is not clearly identified as to be not an ISMS core process the author of this thesis will not use this process as part of the ISMS core processes.

The information security governance process was identified by 24% of the asked experts as an ISMS core process. An explanation could be that the majority of the experts identified this process as a management process, which is supposed by the author of this thesis. The remaining 24% of the experts showed also attention for governing information security but misinterpreting this process as an ISMS core process. So the result of the study confirmed that this process is not an ISMS core process, while still necessary a part of the ISMS. So this process is integrated as management process in the ISMS process framework.

As seen in Table 49 – Results of the study to identify ISMS core processes, processes which were clearly identified as not being an ISMS core process are:

- Configuration management process (16%)
- Capacity management process (8%)
- Budgeting and accounting for services process (5%)
- Problem management process (4%)
- ISMS planning process (0%)
- Service level management process (0%)
- Service reporting process (0%)
- Business relationship management process (0%)
- Supplier management process (0%)
- Incident and service request management process (0%)
- Change management process (0%)
- Release and deployment management process (0%)

All of those processes were also identified as not to be ISMS core processes in this thesis. So as a result of the study this processes were confirmed not to be ISMS core processes.

But it is especially interesting that the “configuration management process” is identified by some experts as ISMS core process. This confirms the practical experience of the author of this thesis in a significant number of ISMS projects were a not correct and up to date IT documentation as well as missing information about dependencies of processes, systems and information is cured by the ISMS and with the budget of the ISMS although this is a responsibility of the IT service management system.

Another interesting result is that no expert identified the ISMS planning process as ISMS core process. This clear understanding of ISMS planning as "process" carried out only once the first life cycle of the ISMS was not foreseen by the author of this thesis although it also represents the opinion of the author of this thesis.

As 3 experts named processes regarding the implementation of measures it was recognized that a more precise interface between the ISMS and the measure implementation is necessary. For this another process will be added to the framework: "Security implementation management process (core process) within the optimization of the framework.

8.3 Verification of the method to determine the necessary maturity level

The proposed method to determine the necessary maturity level for ISMS processes was verified within an expert consultation.

The applicability of the method will also be tested practically within a pilot application (see chapter 8.5 Verification of the framework as a whole and the method to determine the necessary process maturity). Based on the results of the expert consultation the framework will be further improved.

8.3.1 Selection of experts

The validation of the method to determine the necessary process maturity level required experts with the following profile:

- University education (ideally a master degree) in process management or process engineering, computer science, information systems, business informatics, or related field;
- At least 5 years of experience in the relevant area with at least 2 years of experience in a decision-making position;

After the identification of 12 suitable experts they were contacted. 7 experts were interested and willing to participate in a workshop:

- 2 ISMS experts (consulting and auditing)
- 3 persons with a decision-making role (CIO, CTO information security officer)
- 2 process experts (six sigma master black belt)

As 5-7 experts were expected to be an ideal workshop size, 7 experts were ideal for the conduction of the workshop.

8.3.2 Workshop preparation

The proposed method to determine the necessary process maturity level as well as the consideration which lead to the development of the method was provided to the experts four weeks before the workshop. Additionally the following questions were provided to the experts which should be answered within the workshop:

1. Are the preliminary considerations which lead to the method correct?
2. Are there additional and relevant aspects which should be considered? If yes: which aspects?
3. Is the questionnaire formulated clearly? If no: where are clarifications necessary?
4. Does the expert has any further recommendations regarding the method?

8.3.3 Workshop conduction

The workshop was conducted in May 2016 in Berlin, Germany within the offices of the PERSICON Corporation. Within the workshop an extensive discussion about the elements of the method was conducted and the specific questions, which were expected to be answered during the workshop, were addressed.

Specifically the following results were planned:

- optional additional preliminary considerations regarding the method (as answer to the second question)
- a consensus decision regarding the correctness of the preliminary considerations (as answer to the first question)
- a consensus decision regarding the applicability of the method
- an agreed list of questions which need to be clarified (as answer to the third question)
- optional additional recommendations regarding the method (as answer to the fourth question)

8.3.4 Workshop results

The following results were achieved within the workshop:

In spite of lively discussion of the preliminary considerations no additional considerations regarding the method turned out. The lively discussion was the critical success factor to achieve consensus regarding the correctness of the preliminary considerations and the applicability of the method which was also a result of the workshop.

No questions were named by the experts to be removed or added from/to the questionnaire.

A main result of the workshop was a recommendation regarding the clarification of the questions – more specifically the possible answers – about the process performance objectives:

As recommended by the experts it is necessary to obtain comparable and objective answers regarding the questions about the process performance objectives. For this it could be a good method to rate the importance of the five core performance objectives – speed, flexibility, costs, dependability and quality – with importance points at a scale from 0 (not important) to 5 (highest importance). A total of 15 points can be assigned. As a result the importance can be visualized with a spider web diagram as shown as an example in Figure 9 – Importance of process performance objectives.

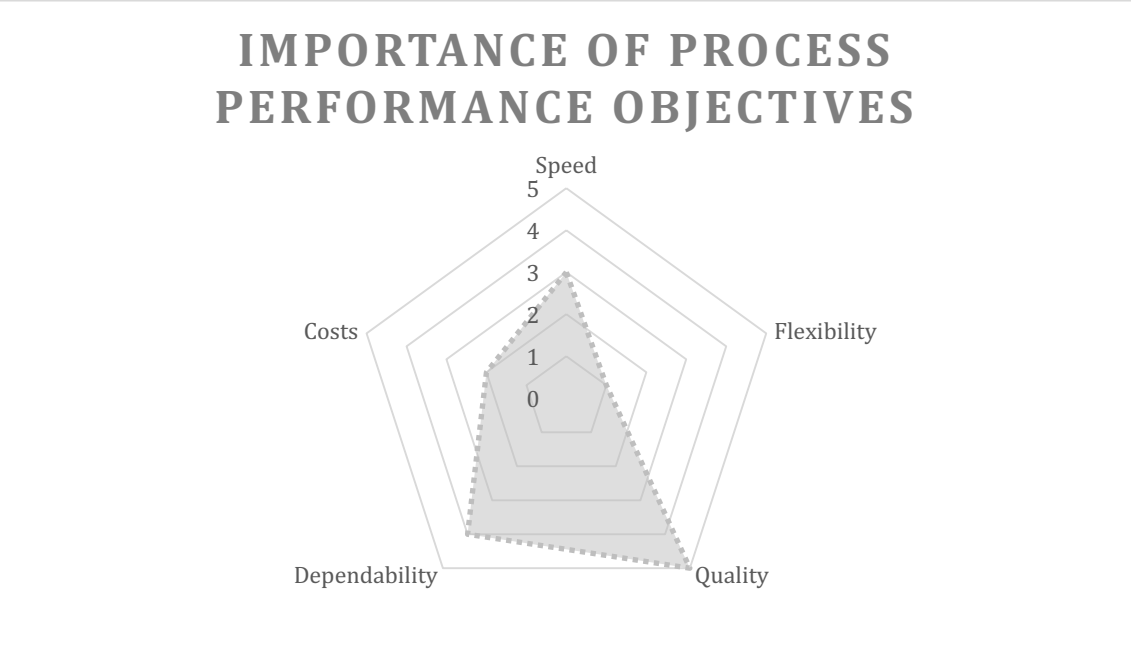

Figure 9 – Importance of process performance objectives

Regarding the question of the dependability of the performance objectives of the process and the relationship to the organizations objectives and vision should be expressed with a predefined scale to allow comparable and objective answers. This scale could be for example:

- 0 – no dependency
- 1 – weak dependency
- 2 – medium dependency
- 3 – strong dependency
- 4 – very strong dependability
- 5 – critical dependability

8.4 Optimization after verification and evaluation

The expert consultations provided a range of insights into improving the ISMS core process framework and the method to determine the necessary maturity level of the ISMS core processes.

In the following, the consideration of these insights is described for the specific processes of the framework. Furthermore, the new version of the framework and the method to determine the necessary maturity level which implements the improvements are presented.

8.4.1 Optimizing the ISMS core process framework and the method to determine the necessary maturity level

8.4.1.1 Optimizing "documents and records control process"

As identified in the expert consultation the documents and records control process does not differentiate enough of requirement documents like policies and standards on one side and records on the other side. The control of records seems more supportive than a core competency of the ISMS, while the control of requirement documents is a core competency of the ISMS. For this the "Documents and records control process" is divided into two processes:

- "Security policy management process" (ISMS core process) – adapted from (Veiga & Eloff, 2007)
- "Records control process" (Supportive process)

8.4.1.1.1 Security policy management process

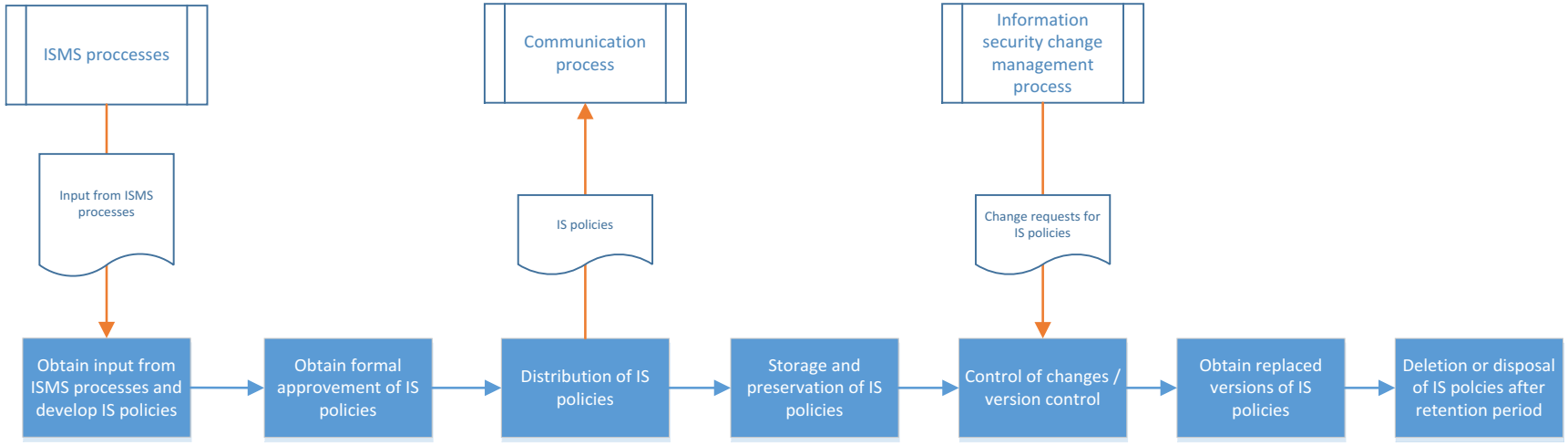

Figure 10 – Security policy management process chart

Process Name	Security policy management process – derived mainly from (Veiga & Eloff, 2007)
Process category	ISMS core process
Brief description	The Security policy management process is the process to develop, maintain and retention of information security policies, standards, procedures and guidelines (in the following named as "IS policies").
Objectives/purposes	Ensure that appropriate policies, standards, procedures and guidelines (IS policies) regarding information security are developed, maintained and available and understood by the target group.
Input	• From ISMS planning process: – ISMS documentation framework including a summary of requirements for ISMS documentation – Established administrative procedure of ISMS document management – Repositories and templates for required policies, standards, procedures or guidelines of the ISMS • All output from other information security risk assessment and treatment process (as basis for policies) • From change management process: necessary changes of policies • From requirements management process: retention requirements
Output	• For all ISMS processes: Appropriate IS policies
Activities/functions	• Obtain input from ISMS processes and develop IS policies • Obtain formal approval of IS policies • Distribution of IS policies (via communication process) • Storage and preservation, including preservation of legibility • Control of changes/version control • Obtain replaced versions of IS policies • Deletion or disposal of IS policies after retention period
Metrics	• Number of changed and re-communicated IS-policies per period • Number of disposed IS policies • Number of documents which initially not fulfill the requirements of the ISMS documentation framework • Number of templates
Owner	Information security officer
Manager	Information security officer
Actors	Information security officer Change management Control implementers Public relations or communications department

Table 50 – Security policy management process

8.4.1.1.2 Records control process

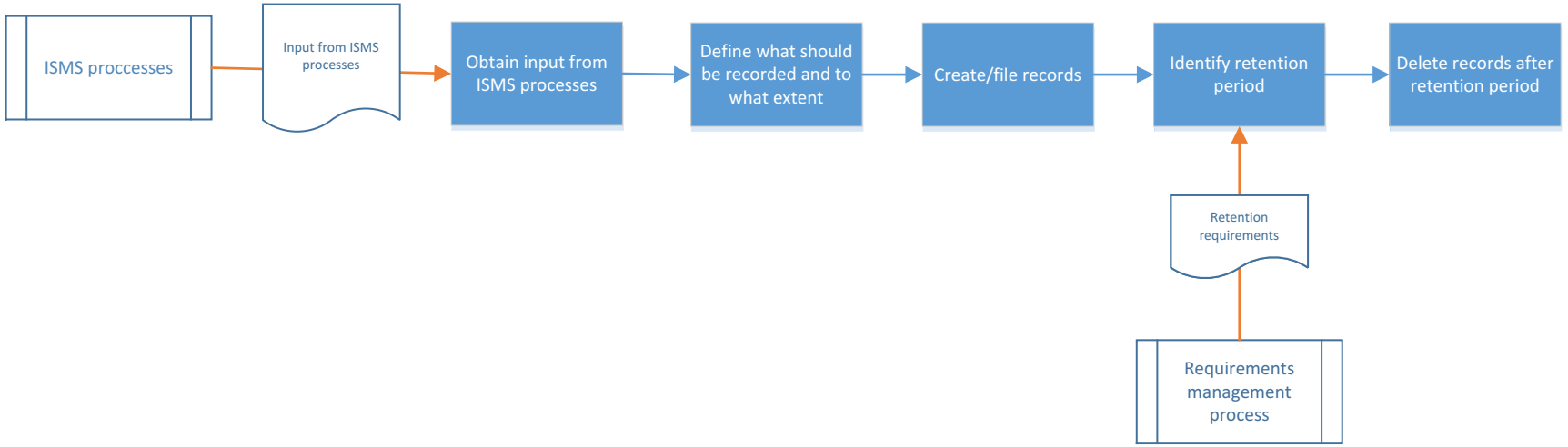

Figure 11 – Records control process chart

Process Name	**Records control process – derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013)**
Process category	Supportive process
Brief description	Records control process is the process to identify, create, update and control information determined to be necessary for the effectiveness of the ISMS.
Objectives/purposes	• Ensure that all information determined to be necessary for the effectiveness of the ISMS are documented and recorded • Ensure appropriate identification, description, format, review and approval for suitability and adequacy of records • Ensure that the relevant recorded information is available for use, where and when it is needed and it is adequately protected • Records are protected from loss, destruction, falsification, unauthorized access and unauthorized release
Input	• From ISMS planning process: – ISMS documentation framework including a summary of requirements for ISMS records control – Established administrative procedure of ISMS records management – Repositories and templates for required records of the ISMS • All output from other information security risk assessment and treatment process (as basis for documentation – for example from information security risk treatment process: records of the results of implementation) • From requirements management process: retention requirements
Output	• For all ISMS processes: necessary records
Activities/functions	• Obtain input from ISMS processes • Define what should be recorded, to what extent • Create/file records • Identify period of retention (partially available as input from the requirements process) • Delete records after retention period
Metrics	• Number of disposed records • Number(s) of records
Owner	Information security officer
Manager	Information security officer
Actors	Information security officer Change management Control implementers Public relations or communications department

Table 51 – Records control process

8.4.1.2 Security implementation management process

As a result of the expert consultation was the insight that a more precise interface between the ISMS and the measure implementation is necessary, another process will be added to the framework: “Security implementation management process (Core process).

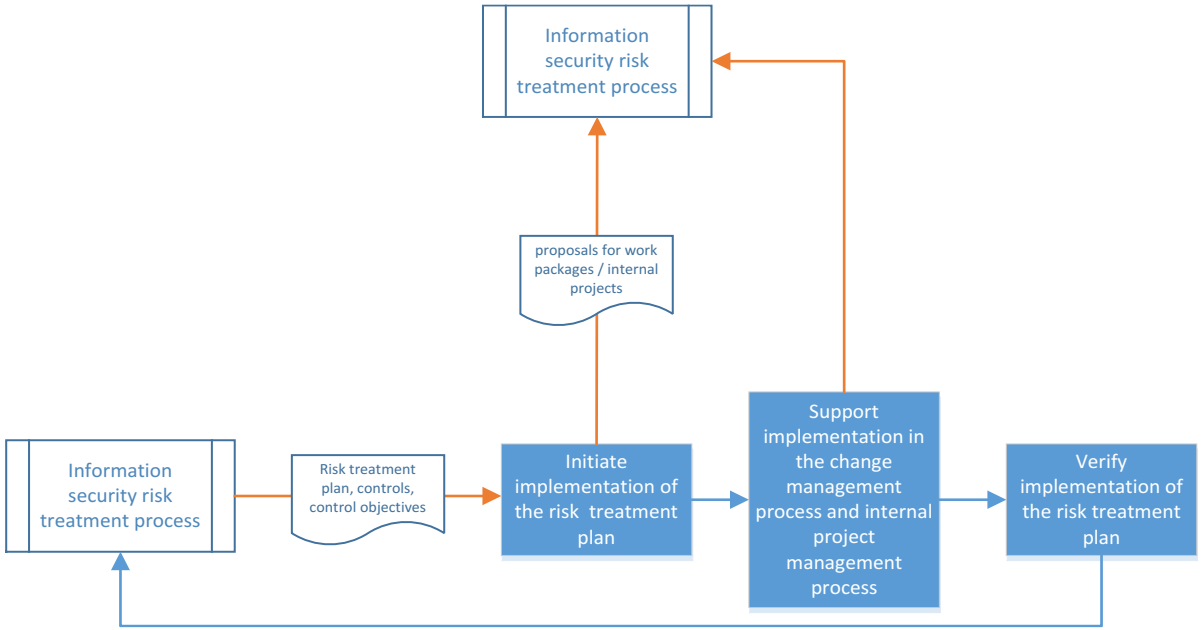

Figure 12 – Security implementation management process chart

Process Name	Security implementation management process
Process category	ISMS core process
Brief description	The security implementation management process is the process to initiate and verify the implementation of the risk treatment plan.
Objectives/purposes	Ensure that the risk treatment plan is executed as planned.
Input	• From information security risk treatment process: risk treatment plan, controls and control objectives • From change management process and/or internal project management process: status regarding implementation
Output	• For change management process and/or internal project management process: proposed changes and control implementation plan
Activities/functions	• Initiate implementation of the risk treatment plan – define and prioritize proposals for work packages / internal projects – perform workshops with asset owners and/or necessary departments (for example IT, facility management, personnel management, etc.) regarding work packages and internal projects and ensure understanding of accountability and responsibility of the asset owners. • Support implementation in the change management process and internal project management process in the role as a stakeholder • Verify implementation of the risk treatment plan
Metrics	• Number of implemented elements of the risk treatment plan • Ratio between planned and realized elements of the risk treatment plan • costs regarding the implementation of elements of the risk treatment plan
Owner	Information security officer
Manager	Information security officer
Actors	Information security officer Change management Control implementers Asset owners

Table 52 – Security implementation management process

8.4.1.3 Including the maturity level determination in ISMS planning process

The task of the determination of the necessary maturity levels of the ISMS processes also needed to be integrated in the framework itself to ensure consistency of the approach. As this task is highly influencing the design of the ISMS it needed to be integrated first in the ISMS planning process. In this process it could be part of the already defined task "Conducting organizational analysis and analysis of information security requirements". As the organizational analysis does focus on the understanding of the organization and its context as well as on the understanding of the needs and expectations of the interested parties (according to (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 1)) the determination of the of the necessary maturity levels of the ISMS processes belongs to the determination of "external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system" (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 1). As a result of this, it was decided that no separate task/step in the already defined ISMS planning process is necessary.

The determined necessary maturity levels of the ISMS processes also needed to be questioned regularly. Needs and expectations regarding the process maturity levels can change. Changed necessary maturity levels of ISMS processes need to be considered within the information security improvement process in which the ISMS processes itself are one target of improvement. As a result on this process also no modifications were necessary.

8.4.1.4 Low maturity level ISMS core process framework

Often management systems are implemented with an iterative approach (Eloff & Eloff, 2003; Vuppala, Vincent, Kusler, & Davidson, 2011) and not at one time. Also iteration is included in ISO 27001 in form of the regularly improvement (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 9). Practical experience of the author of the thesis also showed, that initial ISMS implementation projects are regularly long lasting projects between one and two years. Questions regarding a step by step approach arise regularly from the stakeholders. Given this and considering the method to determine the necessary ISMS process maturity levels it is obvious to think about maturity iteration steps regarding the ISMS design and implementation. The question is: Are there ISMS processes, which are generally only necessary at higher maturity levels? If so, what would be the remaining basic ISMS core process framework at a lower than maturity level 4 (predictable process). To answer this question all processes were analyzed regarding the identification of processes which were relevant mostly at higher maturity levels.

As a result the dismissing the following processes in an ISMS framework with a generally maturity level lower than level 4 will be discussed:

- Internal audit process – The objective of this process is to examine the effectiveness and efficiency of the ISMS and implemented controls independently within the scope of internal audits (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 55). Results of this process are primarily used to improve the measures or the ISMS processes. Improvement is a requirement of maturity level 5 and corrective actions are primarily used to ensure that a process operates predictively within defined limits to achieve its process outcomes (maturity level 4). As a result, the internal audit process would be generally necessary only in maturity levels higher than 3.
- Performance evaluation process – The performance evaluation process contains monitoring, measurement, analysis and evaluation of two main criteria. First, the performance of the security controls and second the performance of the ISMS processes. Performance measurement differs from performance audit (internal audit) which is performed independently. As a result the considerations about the internal audit process are also applicable to the performance evaluation process.
- Information security improvement process - Objective of this process is to ensure and improve a continuing suitability, adequacy and effectiveness of the ISMS. This is only necessary at the process maturity level 5: Innovating process were predictable processes are continually improved to respond to changes aligned with organizational objectives. As a result this process would generally only be necessary at maturity level 5.
- The information security customer relationship management process and information security governance process ensure the alignment of the ISMS process outcomes with the expectations of the stakeholders and customers. Based on the experience of the author of this thesis this is usually from general interest, but a low (described by the management as informal) maturity level of the information security governance processes would still be necessary. As a result only the process of information security customer relationship management should be dismissed generally in lower overall maturity levels of the ISMS.
- Information security change management process – This process deals with changes of the ISMS processes as well as the information security measures. Were the controlled changes of ISMS processes with the improvement of the ISMS could be only necessary at higher maturity levels, the control of changes regarding the information security measures is also necessary at lower maturity levels. As a result this process cannot be dismissed at lower maturity levels.

The resulting basic framework is shown in Figure 13 – Basic ISMS process framework for generally low maturity requirements.

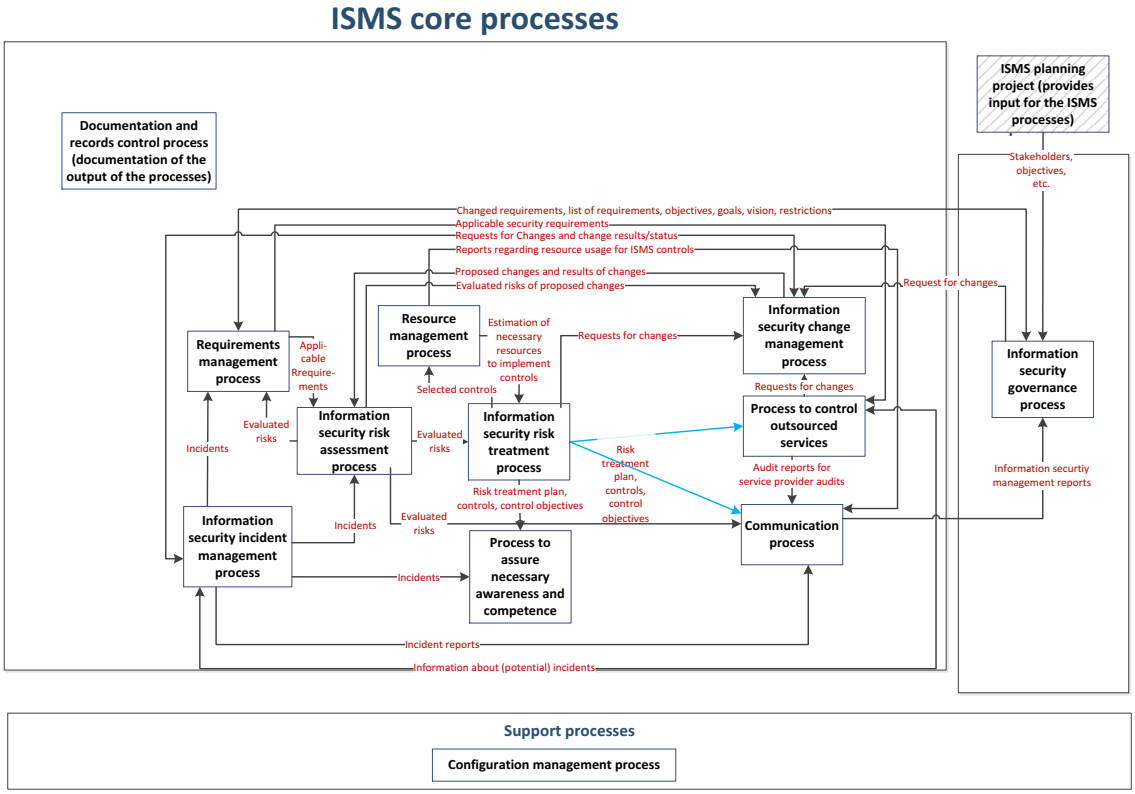

Figure 13 – Basic ISMS process framework for generally low maturity requirements

According to Buglione and Abran (2006) "a few studies have investigated the maturity level equivalence for those organizations already ISO 9001:2000-certified and implementing CMMI or SPICE processes between maturity levels 2 and 3 (Paulk, 1993), and they have raised a few issues. For instance, an ISO-certified organization must – to be certified – demonstrate that they have a process in place to identify and eliminate the causes of non conformities…"

Also the dismissed processes of internal audit, performance evaluation and improvement are stipulated in the ISO 270001. Therefore a certification of the basic ISMS process framework – without any maturity level of the dismissed processes – would not be possible. As the solution the dismissed processes should not be dismissed completely, but implemented at a low maturity level.

8.4.2 Optimization of the method to determine the necessary maturity level

Based on the results of the expert consultation the answers regarding the questions about the process performance objectives as well as regarding the dependability of the performance objectives of the process and the relationship to the organizations objectives and vision were clarified as follows:

Criteria	Questions	comments
Questions regarding process performance objectives **Please rate the importance of the five core performance objectives – speed, flexibility, costs, dependability and quality – with importance points at a scale from 0 (not important) to 5 (highest importance). A total of 15 points can be assigned.**		
Importance of process result quality	How important is the quality of the process results?	The higher the demanded quality of process results, the higher the maturity of the process should be.
Importance of processing speed	How important is a processing time?	If speed is the primary goal of the process, processing time needs to be measured continually. This could be an indicator of maturity level 4 or even level 5.
Importance of process flexibility	How necessary is it to ensure a flexibility of process steps? What degree of flexibility is needed?	If flexibility is the primary goal of the process it seems not sufficient to define every alternative path of the process. So this would be an indicator for maximum maturity level 2.
Importance of process costs	How important is it to ensure minimum costs of process operation?	Minimum costs could be an indicator for a low process maturity as process overhead costs will rise with a higher process maturity. However, this is also dependent on the necessary quality of process results. Where a high process result quality is required, it could be necessary to rise the process maturity to avoid costs resulting from poor quality of process results.

Criteria	Questions	comments
Dependability	How does the performance objectives of the process relate to the organizations objectives and vision? Which objectives and vision are influenced by the process and/or process results? please use the following scale to express the dependability: • 0 – no dependency • 1 – weak dependency • 2 – medium dependency • 3 – strong dependency • 4 – very strong dependability • 5 – critical dependability	The more depended the objectives of the organization (and the more important the objectives are) are form the process or process output the higher the maturity of the process should be.

Table 53 – Changed process maturity criteria and questions

8.4.3 Summary of the optimization

As a result of the improvements of the framework and the method to determine the necessary maturity level the optimized framework is shown in Figure 14 – Optimized ISMS process framework and the optimized method is shown in Table 54 – Optimized process maturity criteria questionnaire.

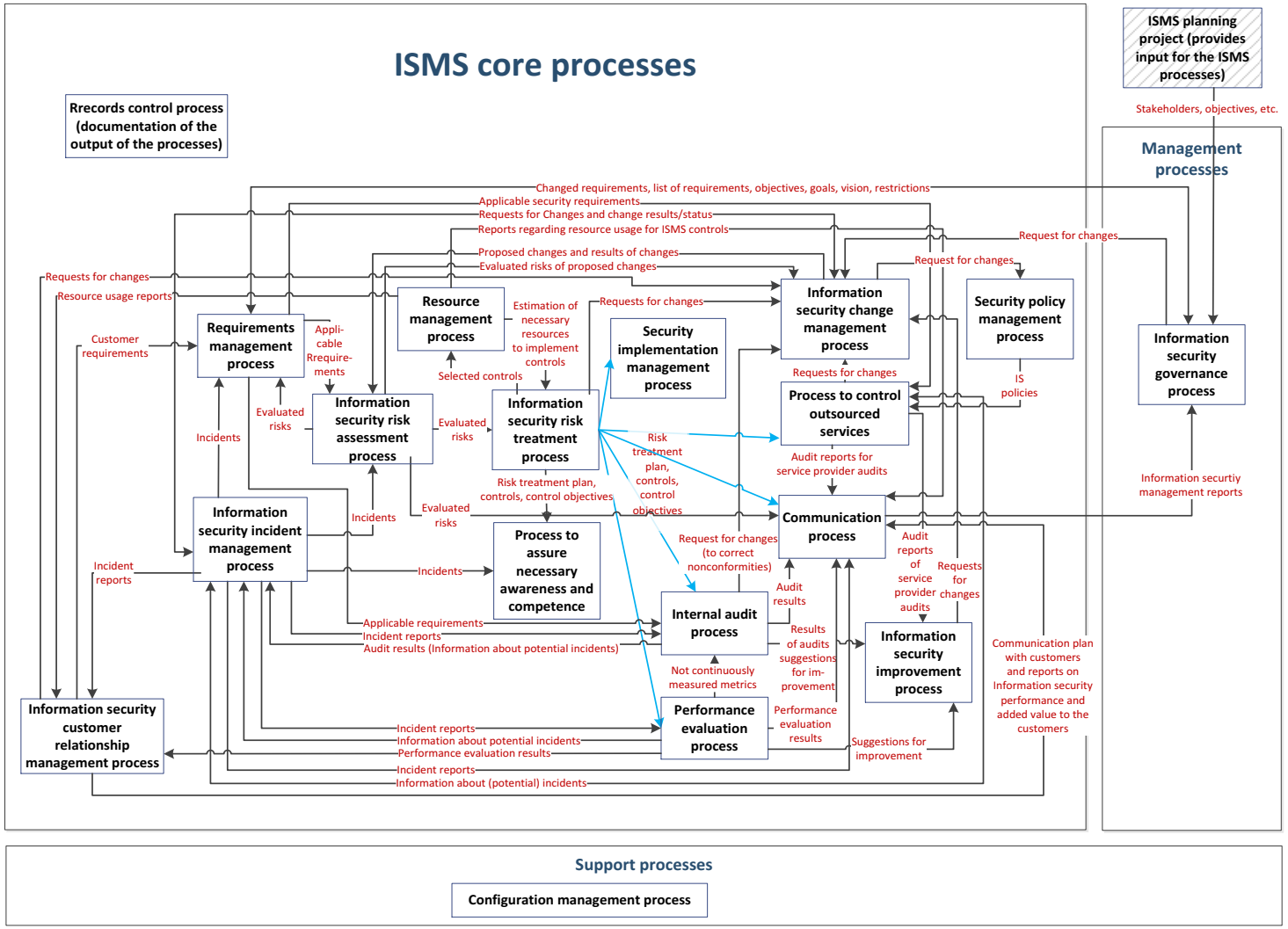

Figure 14 – Optimized ISMS process framework

Criteria	Questions	Comments
Questions regarding the organization – to be answered only once for an organization		
Organizations objectives and vision	What are the objectives and the vision of the organization?	This is necessary to later analyze how the performance objectives relate to the organizations objectives and vision.
Industry classification	What is the industry classification of the organization? For example: • Capital-intensive industries, other than utilities (Cap) • Utilities (Util) • Service industries (Srv) • Financial institutions (Fin) • Government and non-profits (Govt)	An ISACA study found that the industry classification statistically influences the maturity of the processes (Information Systems Audit and Control Association, 2008, p. 66).
Size of IT operations	What is the size of IT operations taking into account: • IT staff members • Application systems • Clients?	An ISACA study found that the size of the IT operations generally influences the maturity of the processes (Information Systems Audit and Control Association, 2008, p. 66).
Maturity level of core business processes	What is the maturity level of the core business processes?	Mature business processes could be an indicator for the general demand of mature processes (also depending on the size, business model, sector, location). The maturity of the information security program is influenced by the maturity of the organization which is linked to the degree systemic thinking is used in the organization. Systemicthinking paves the way for systemic processes. (Information Systems Audit and Control Association, 2009, pp. 10, 11)
General process specific questions		
Current maturity level of the process	What is the current maturity level of the process?	This is necessary as starting point to analyze later if it is possible to increase or decrease the process maturity.
Complexity of the process	How complex is the process? How many decisions and alternative paths does the process contain?	Complex process flows with multiple alternative paths generally require a higher process maturity (at least level 3) to ensure reliability of process results and to reach process objectives.

Criteria	Questions	Comments
Degree of visibility of the process and/or process results	How visible is the process and the process results to - Stakeholders of the process? - the public?	A high visibility of the process or even more of the process results often results in the need for a higher process maturity.
Questions regarding process performance objectives **Please rate the importance of the five core performance objectives – speed, flexibility, costs, dependability and quality – with importance points at a scale from 0 (not important) to 5 (highest importance). A total of 15 points can be assigned.**		
Importance of process result quality	How important is the quality of the process results?	The higher the demanded quality of process results, the higher the maturity of the process should be.
Importance of processing speed	How important is a processing time?	If speed is the primary goal of the process, processing time needs to be measured continually. This could be an indicator of maturity level 4 or even level 5.
Importance of process flexibility	How necessary is it to ensure a flexibility of process steps? What degree of flexibility is needed?	If flexibility is the primary goal of the process, it seems not sufficient to define every alternative path of the process. Therefore, this would be an indicator for maximum maturity level 2.
Importance of process costs	How important is it to ensure minimum costs of process operation?	Minimum costs could be an indicator for a low process maturity as process overhead costs will rise with a higher process maturity. However, this is also dependent on the necessary quality of process results. Where a high process result quality is required, it could be necessary to rise the process maturity to avoid costs resulting from poor quality of process results.

Criteria	Questions	Comments
Dependability	How does the performance objectives of the process relate to the organizations objectives and vision? Which objectives and vision are influenced by the process and/or process results? please use the following scale to express the dependability: • 0 – no dependency • 1 – weak dependency • 2 – medium dependency • 3 – strong dependency • 4 – very strong dependability • 5 – critical dependability	The more depended the objectives of the organization (and the more important the objectives are) are form the process or process output the higher the maturity of the process should be.
Questions regarding process output and costs		
Variation in demand of the process outputs	Are there specific points in time were process outputs are critical for other processes and/or for reaching organizations objectives and vision?	If there is a great variation in the demand of the process output this could be an indicator that the process is not often performed. So the staff is usually not trained to perform the process. This could be an indicator for the demand of maturity level 3.
Volume of the process output	What is the volume of the process output?	Processes with a high volume of process output are often performed at a high frequency which means that the staff is usually trained to operate the process (indicator, that level 2 would be sufficient) but could also be an indicator for the demand of a higher maturity level – depending on the dependability of the organization from the process results.
Variety of the process output	How many different process outputs do exist? How great is the variety of the process output?	A great variety of a process output could be an indicator of a complex process with multiple alternative paths. Complex process flows with multiple alternative paths generally require a higher process maturity (at least level 3) to ensure reliability of process results and to reach process objectives.

Criteria	Questions	Comments
Costs	How much in terms of money, and work time does one process execution cost?	The higher the cost of the process execution the more it is likely that a high process maturity is required. This is the case because the higher the process costs the more reliability of the process is needed.
Frequency of process operation	How often is the process operated?	A high frequency means that the staff is usually trained to operate the process (indicator, that level 2 would be sufficient) but could also be an indicator for the demand of a higher maturity level – depending on the dependability of the organization from the process results.
Consequences of changing current maturity level		
Costs / Benefits of specific maturity levels of the process	What are the costs to increase the maturity level (for each maturity level left)?	This information is necessary to evaluate if a higher or lesser maturity level of the process could be appropriate.
Costs / Benefits of specific maturity levels of the process	What are the benefits to increase the maturity level (for each maturity level left)?	This information is necessary to evaluate if a higher or lesser maturity level of the process could be appropriate.
Costs / Benefits of specific maturity levels of the process	What are the costs to decrease the maturity level (for each maturity level left)?	This information is necessary to evaluate if a higher or lesser maturity level of the process could be appropriate.
Costs / Benefits of specific maturity levels of the process	What are the benefits to decrease the maturity level (for each maturity level left)?	This information is necessary to evaluate if a higher or lesser maturity level of the process could be appropriate.
Risks	What are the risks to operate the process at specific levels?	This information is necessary to evaluate if a higher or lesser maturity level of the process could be appropriate.
Already communicated or identified requirements regarding the process (dependent also from the industry classification of the organization)		
Legal requirements	Are there specific legal requirements regarding the process or the process results (for example records of the process)?	Already communicated or identified requirements regarding the process are strong indicators for the necessary process maturity.
Customer requirements	Are there requirements of customers to operate the process at a specific maturity level? If so: Which maturity level is stipulated by the customers?	Already communicated or identified requirements regarding the process are strong indicators for the necessary process maturity.

Criteria	Questions	Comments
Management requirements	Are there requirements of the management to operate the process at a specific maturity level? If so: Which maturity level is stipulated by the management?	Already communicated or identified requirements regarding the process are strong indicators for the necessary process maturity.

Table 54 – Optimized process maturity criteria questionnaire

8.5 Verification of the framework as a whole and the method to determine the necessary process maturity

8.5.1 Method

To verify the overall results of the PhD work (framework and method to determine the necessary process maturity) a proof-of-concept implementation respectively a pilot application was chosen. The implementation project started in May 2016 and was finished in January 2017.

The author of this thesis had the role of a project manager (external consultant) regarding the planning and implementation of an ISMS. In that role the author of this PhD thesis spent about 150 person days within that project.

The project plan is provided in Figure 15 – Pilot application – ISMS project plan, were WP stands for work package:

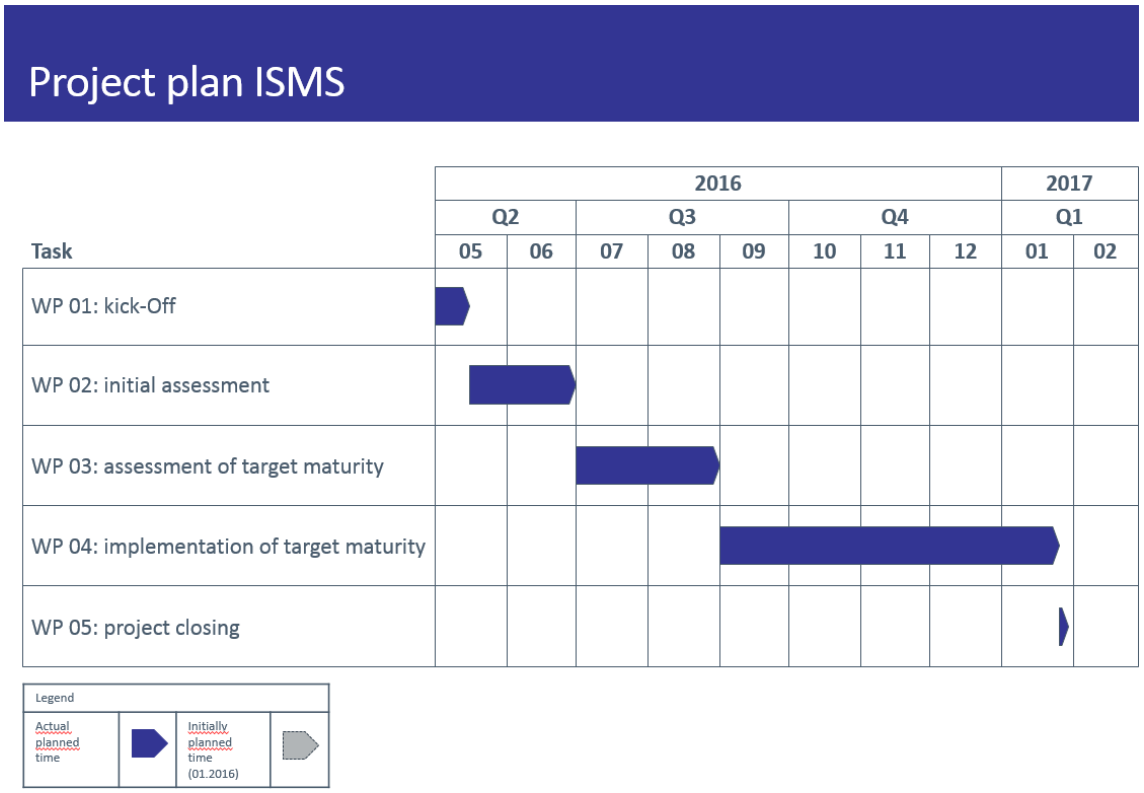

Figure 15 – Pilot application – ISMS project plan

8.5.2 Sample (piloting organization)

The ISMS core process framework has been implemented and is operational in a medium-sized government organization as a pilot project. As confidentiality was agreed with that organization the organization and characteristics of that pilot implementation project are described anonymously were necessary:

The organization is characterized by a high level of outsourced services. Tasks regarding supplier and service provider management are daily routines. The organization consists of about 400 employees on one main facility. An appreciable part of that employees are temporary workers.

In the beginning of the project, there were already substantial ISMS processes in place, but they were not consequently oriented at a standards or even certified, nor were the process maturity levels determined or planned. The actual processes were grown over the years without any structured approach.

8.5.3 Results and discussion of the results

After each work package a lessons learned workshop was conducted with the information security officer of the piloting organization. Results of that lessons learned are discussed in the following.

8.5.3.1 WP 01 Kick Off

WP 01 consists of a kick-off workshop regarding the planned project. Preliminary necessary stakeholders from the management, potential process owners (of processes with interfaces to the ISMS core processes) and stakeholders from the departments (head of divisions) of the organization were identified and participated in the workshop. With that workshop the necessary management attention and commitment was realized as well as participants in the next steps understood the project objectives and their roles in the next steps.

Results/Lessons learned:

Besides explaining the WPs and project objectives a critical success factor was the explanation and understanding the processes and the process framework as a starting point. During the workshop uncertainty as well as rejection was noticeable resulting from the complexity of the framework. The complexity of the framework distracted the information security officer and the other participants from the main idea of process orientation. So special attention must be paid to ensure an open minded workshop climate and to avoid disaffirmation of the project in this early phase. This was realized through explaining the process framework. When realizing that this framework is not generally new and the framework consists of elements which are mainly already in place and are operated in daily routines lost the negative prejudice regarding the framework step by step.

8.5.3.2 WP 02 initial assessment

In WP 02 an initial assessment of the actual process maturity was conducted by the author of this thesis in the role of an external auditor. A checklist and interviews with process managers/owners was used within this task. As a result the actual maturity level of the ISMS core processes was determined objectively.

The results of this initial process maturity assessment are shown in Figure 16 – Pilot application – actual ISMS process maturity.

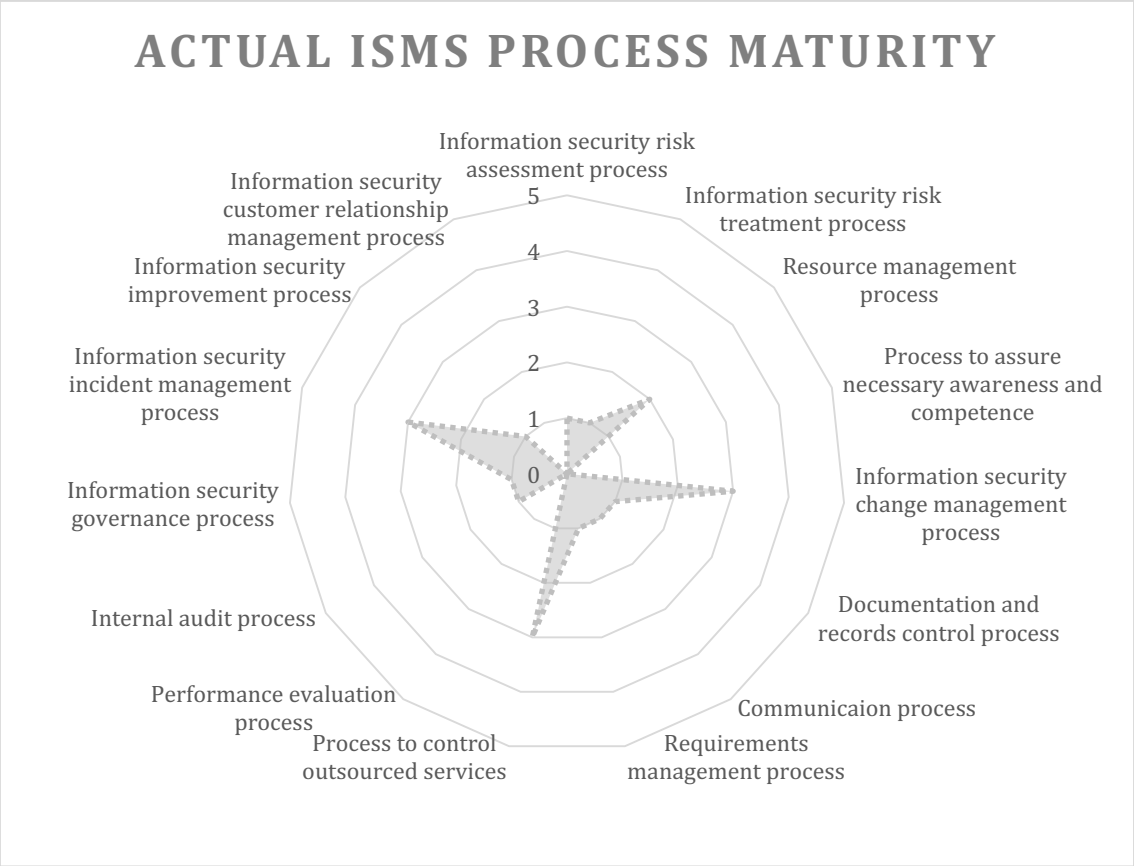

Figure 16 – Pilot application – actual ISMS process maturity

Results/Lessons learned:

Determining the actual process maturity objectively was especially useful for the next step as the supposed process maturity (as determined in a self-assessment from the CISO) differed for some processes from the existing maturity level. From the viewpoint of the author of this thesis and considering his experience as an auditor for information security, this is an effect which is often present. CISOs tend to overvalue the present process maturity of their processes (optimistic, not repeatable and not objective according to (Information Systems Audit and Control Association, n.d.-e, p. 8).

8.5.3.3 WP 03 assessment of target maturity

In WP 03 the assessment of the target maturity level was performed using the method described in chapter 7 Method to determine the necessary maturity level. An example of the results and their analysis of the target maturity level questionnaire is contained in Appendix H – Pilot application – Target process maturity analysis – Process to control outsourced services .

Figure 17 – Pilot application – actual and target ISMS process maturity shows the overall results of the target maturity level analysis compared to the actual status of the ISMS process maturity levels.

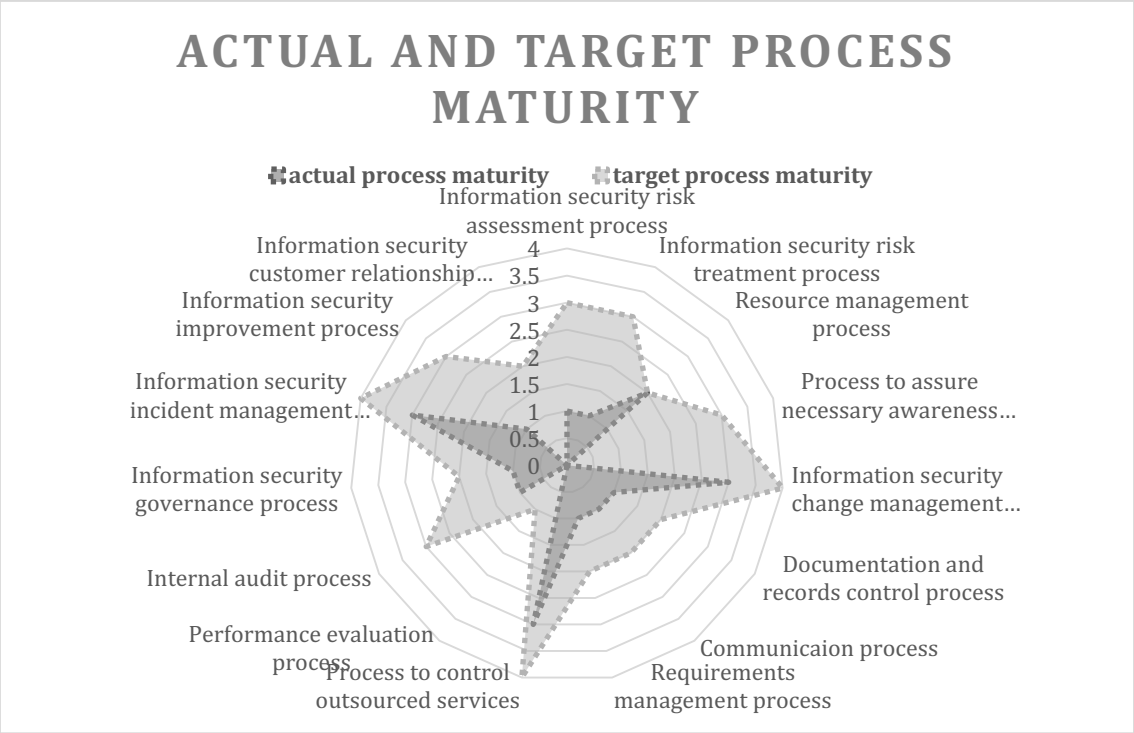

Figure 17 – Pilot application – actual and target ISMS process maturity

Results/Lessons learned:

While obtaining answers to the questionnaire especially cost information (costs to perform the process or to raise to other maturity levels) were difficult to estimate. A qualitative scale instead of estimating monetary resources in form of euros could be a solution, but would also result in a lower comparability as the qualitative scale must be well defined. Another lessons learned of this step was, that the application of the method to determine the necessary maturity level of the ISMS processes made the potential benefits and risks of every process in general and more specific for each maturity level of the processes transparent and clear to all involved persons.

8.5.3.4 WP 04 implementation of target maturity

After determining the target maturity of every ISMS core process the gaps between the actual process maturity levels and the target maturity levels were closed in WP 04. Processes, where quick improvements of the process maturity were possible, were prioritized to ensure fast, visible and noticeable project results. In information security projects analysis phases are often stressed and take a major part in the projects. But analyzing does not change the reached security or maturity level. So special attention was paid to produce noticeable changes as fast as possible.

Results/Lessons learned:

During this stage, a major lesson learned was, that an unmodified application of the ISMS process framework is not suitable. ISMS processes need to be tailored to the specific needs of the organization, but are of great value as a starting point. Starting with a proposed ISMS process framework results generally in focusing on a process perspective rather than a measure perspective (one major feedback from the information security officer of the piloting organization). This is especially helpful because risks of a measurement driven approach like the understanding of information security as a one-time project are avoided and replaced by a process oriented view which better fulfills the requirement of operating an ISMS. An ISMS process framework as a starting point also prevents the implementing organization from researching the standards regarding ISMS processes, as they are already provided.

Regarding the process to control outsourced services for example, it turned out, that important interfaces with the information security incident management process and the change management processes were necessary in this particular application. As information security incidents from the service provider will influence the information security of the services provided and taking into account the strong dependability of the organization from the reliability and security of those services, some major modifications of the process proposed in the framework were necessary. Also a strong integration of the information security incident management process of the service provider and the outsourcing organization were necessary. Additionally regulative notification requirements to regulating authorities needed to be planned and implemented.

Figure 18 – Pilot application – information security incident handling process as part of the process to control outsourced processes shows the resulting process part regarding the handling of security incidents of the service provider as part of the process to control outsourced services. This strong modification to the proposed process in ISMS core process framework were necessary, but, in the opinion of the author, this should not be implemented in the ISMS core process framework, as the requirements of the piloting organization are too special regarding this particular aspect.

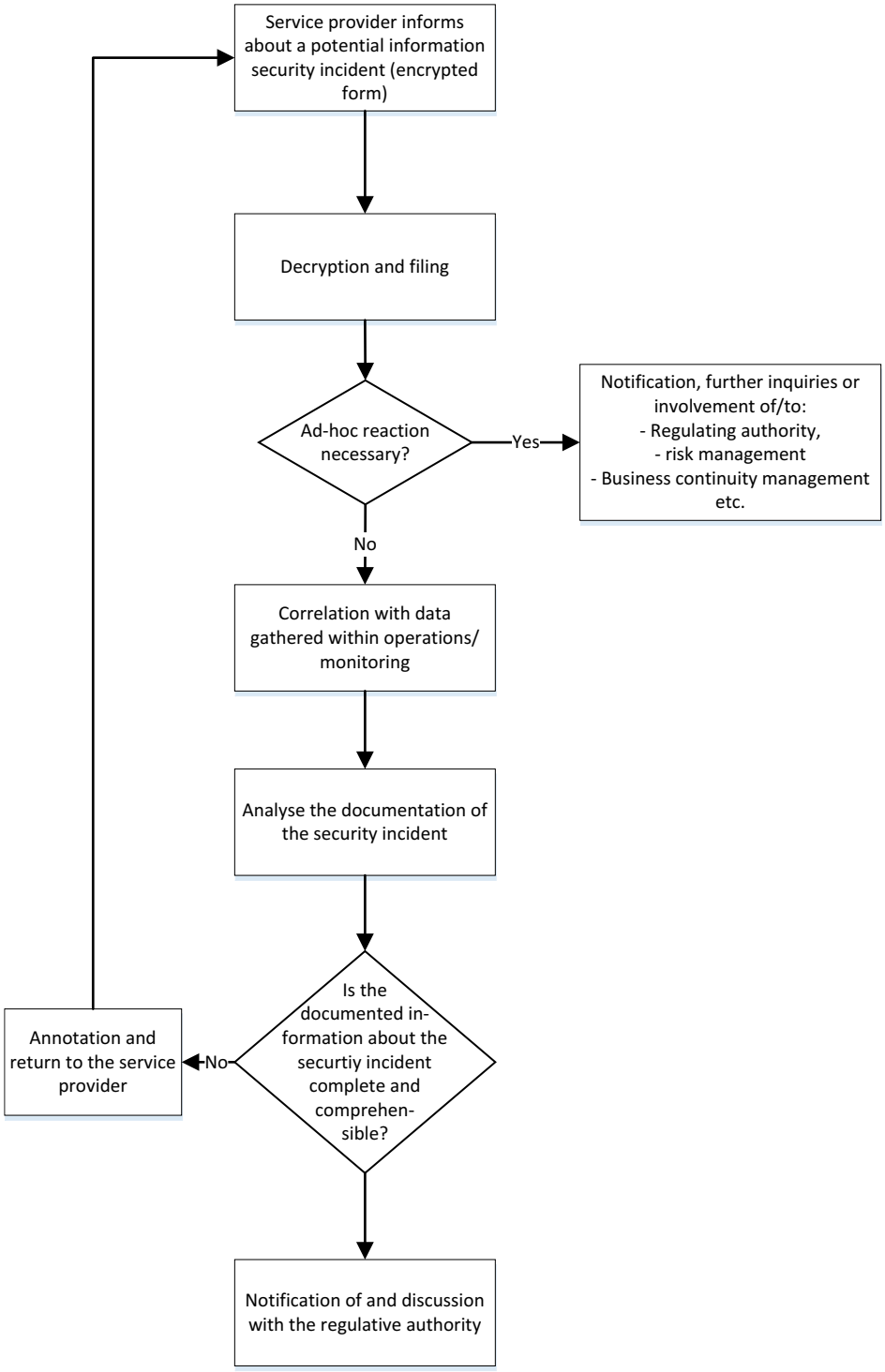

Figure 18 – Pilot application – information security incident handling process as part of the process to control outsourced processes

Another major aspect learned during the planning and implementation of the target process maturity levels was, that security policies are of major importance regarding the visibility of the ISMS within the organization. As a result special attention was paid to ISMS policies by the implementing organization.

Another major challenge was to initiate the information security measures identified within the information security risk treatment plan. Especially challenging was the discussion with the stakeholders regarding the questions:

- Who is accountable/responsible for the implementation of the measures?
- Who will finance the measures?

8.5.3.5 WP 05 project closing

WP 05 consisted the project closing including a final lessons learned session. Lessons learned sessions were also performed after the completion of every WP.

Results/Lessons learned:

Beside the modification of the ISMS processes to fit the individual requirements of the organization, processes differ in the implemented maturity level. Especially the process to control outsourced services and the information security incident management process needed to be implemented at a high maturity level in the piloting organization due to a significant dependability on the provided services.

Some processes were not necessary at maturity levels of “defined” or higher in the piloting organization. Examples are internal audit process, performance evaluation process, information security improvement processes. Beside the individual requirements of the piloting organization the organization decided to initially implement only the most important processes from their point of view as a starting point.

8.5.3.6 Discussion

In this section results from the case study will be compared to relevant literature as identified in chapter 6.2 SLR – Analysis of the latest research regarding maturity level model use within an ISMS.

To sum up the evaluation results of the pilot application, implementing the proposed ISMS process framework has the following advantages compared to the traditional measurement or control-objective-driven approach from the viewpoint of the author of this thesis as well as from the viewpoint of the piloting organization (ISO and management were questioned about that and confirmed this):

- Efficiency – the implementing organization does not need to research possible ISMS processes in the ISO standards, as they are provided within the framework. The author of this thesis spent about 5 work days per ISMS process for researching the standards and deriving the process chart and the process profile information. Given the 15 ISMS core and management processes, a minimum of 75 work days for research can be saved by every implementing organization. According to (Benner & Tushman, 2003) organizations learn and increases their efficiency through repetition. As a result of this, process management focus on improving an organizations efficiency according to Benner and Tushman (2002). By implementing the ISMS processes at specific, demanded maturity levels a total sum of 40 maturity levels where necessary. Starting with a total sum of 19 maturity levels in simple terms the maturity was nearly doubled within the case study. Otherwise the implementing organization saved resources for 5 maturity levels compared to a scenario in which every process is implemented at a minimum maturity level of 3, which was a former objective of the organization.
- Operational focus – According to Becker and Kahn (2003) in recent decades, organizations have oriented to an efficient execution of functions (or controls), which has led to a local optimization and perfection of functional areas or controls. (Becker & Kahn, 2003) also identified, that a focus on cross-functional business processes is required. Also Mitasiunas et al. (2014) stated, that dedicated security-focused processes must be defined and implemented. Given the process-based view of security, related process capability needs to be continuously evaluated and improved according to Mitasiunas et al. (2014). By implementing the ISMS process framework within the case study, the focus of the implementing organization was shifted from control objectives to a process oriented view, which better enables and supports an operation of an ISMS. Also the differentiation between ISMS operation and controls turned out to be very beneficial, as it was more transparent now to the involved persons, which role is accountable or responsible for what. Especially the insight, that the ISMS is not responsible nor accountable for defining security requirements and for funding specific controls, grew over the time. Moreover the insight grew, that the ISMS team is offering services which helps the asset owners to achieve and maintain an adequate security level.

- Benefits and transparency – According to O-ISM^3 (The Open Group, 2011) it is necessary to give management the tool for identifying which benefits ISMS gives to the organization, which processes can be improved and in what extent." Results of the case study showed, that the benefits of the ISMS processes and the ISMS itself were made transparent in the WP 03 f the case study. WP 03 also resulted in information about which processes can be improved and in what extent, which led to more efficiency by focusing limited resources on processes, where increasing the maturity is most beneficial.
- Ranking and benchmarking - According to Coelho et al. (2014) there is a great demand for a tool which is able to demonstrate the maturity level of an information security system. As a result of the case study, the implementing organization was able to demonstrate the adequacy of the maturity level of every ISMS process and as a result of that the maturity level of the ISMS itself. By making the maturity level of the ISMS and ISMS processes transparent benchmarking and ranking of organizations according to the ISMS or ISMS-process maturity levels would be possible and beneficial for example by identifying and choosing possible service providers. Benchmarking in general would be possible, because the proposed ISMS process framework as well as the maturity levels are formulated in a general manner to fit for all organizations independent of their size, objectives, business model, location et cetera. Nevertheless, Eshlaghy et al. (2011) found out that no research has been performed about ranking organizations based on the level of the information security maturity, till yet. This would also be an option for future research.

Part V – Conclusions

9 Conclusions and outlook

This chapter addresses the assessment of the accomplishment of the postulated objectives, a list the main contributions of the thesis and the benefits that the proposed framework can provide to organisations. In this chapter also potentials for future applications and further development of the framework as well as an outlook on future research activities in the area are discussed.

9.1 Accomplishment of Objectives

In this thesis an ISMS core process framework as well as a method to determine the necessary maturity level for ISMS processes was developed and verified within expert studies as well as tested in a real world organization setting within a pilot application.

The following research objectives have been accomplished:

1. ***Objective – Develop an ISMS core process framework***

This objective was accomplished by analyzing existing standards as well as performing a SLR, an expert consultation and a pilot application. Based on this an ISMS core process framework was developed and optimized. An evaluation if the proposed process framework is a process framework according to ISO 33004 is contained in Appendix I – Evaluation of the ISMS process framework against ISO 33004.

2. ***Objective – Select or modify an existing maturity level model for the use with the ISMS core process framework***

This objective was accomplished by analyzing existing standards as well as performing a SLR. As a result an existing maturity level model of CMMI identical with ISO 15504 was chosen for the use with the ISMS core process framework.

3. ***Objective – Develop or identify a method to determine the necessary maturity level of ISMS core processes***

This objective was accomplished by analyzing existing standards and literature, an expert consultation and a pilot application. Based on this a method to determine the necessary maturity level of ISMS core processes was developed and optimized.

4. ***Objective – find a proper method to evaluate and validate assumptions with experts***

This objective was accomplished by performing several expert consultations as described in chapters 5.2 as well as chapter 0.

9.2 Main contributions

The main contributions of this work are summarized as follows:

1) This thesis includes state of the art analysis of ISMS processes as well as regarding the use of maturity level models within ISMS. This is a valuable foundation for future research in the area.
2) The thesis also includes a process oriented mapping of the established ISMS standards (ISO 27000 series, COBIT and ISO 20000-1/ITIL), which is a valuable foundation for future research in the area.
3) The presented atomized requirements of the ISO 27001 as well as the mapping of the requirements to process areas will help practitioners to design, implement and operate an ISMS. It will also support practitioners as well as auditors as a checklist.
4) The thesis contains a reduction of 142 requirements from ISO 27001 as well as 28 process candidates, which were compiled and arranged in a framework of 17 ISMS core processes. So the complexity was reduced and the requirements regarding the operation of an ISMS were clarified.
5) The definition of what is a core process of the ISMS can be used as a blueprint to differentiate responsibilities and accountabilities within the domains of an integrated management system.
6) The verification of the framework and the method to determine the necessary maturity level demonstrates the relevance of the topics of this thesis in the industry.
7) The evaluation of the framework in a real-world scenario provides a proof of the applicability and adaptability of the framework.

9.3 Benefits of the proposed framework and the method to determine the necessary process maturity

The benefits of the proposed framework as well as the proposed method to determine the necessary maturity level for ISMS processes are summarized as follows: The framework provides a process and operations oriented approach to information security management, were the method to determine the necessary maturity levels ensures efficient use of limited resources.

More specifically the benefits are

1) The proposed framework provide a detailed but generic blueprint regarding the core processes an ISMS consists of. The framework is applicable to all organizations independent of their size, objectives, business model, location et cetera. The ISMS core process framework as a prototype for an ISMS.
2) The process orientation of the framework supports the transition from designing and implementing an ISMS (project phase) to the operation of the ISMS (performing the processes), which is a main problem in real life applications.
3) The differentiation between measures and ISMS processes
4) The process orientation also supports and allows the integration of the ISMS processes in further domains of an integrated management system.

5) The presented method to determine the necessary maturity level for ISMS processes can be used to tailor the framework to individual requirements and based on this to ensure appropriateness and efficiency of the individual implementations of the ISMS.
6) The expert verification demonstrates that the framework and the method was met with a good degree of acceptance by leading practitioners in the field.
7) The evaluation approach can serve as a guide for the introduction of the framework in organizations.

9.4 Critical reflection and lessons learned

When planning the thesis and necessary steps regarding the research the complexity and effort was underestimated. Plans that were set out at the beginning needed adaptations to consider unexpected outcomes - for example the limited results from the SLR regarding the analysis of the latest research regarding maturity level model use within an ISMS.

Based on the decade-long experience of the author as an expert in the field of information security management, some early expectations about the ISMS processes needed to be revised – for example the process of information security customer relationship management was not expected as an outcome at the beginning of the research. Recognising the relevance of the framework from a pragmatic and user-oriented point of view, the author had to dive deep and conduct several workshops with the supervisors in order to establish a solid understanding of how to prepare the necessary research steps and to present the results properly. The state-of-the-art in information security management is also developing faster and faster. New ISO standards in the ISO 27000 family are approaching every year. While this may serve as a proof about the foresight to select a topic with a growing relevance that is “cutting-edge”, it also required several periodic updates of the background section in order to reflect developments that emerged worldwide during the development, validation, and evaluation of the framework and the method to determine the necessary maturity levels for the ISMS processes.

This duality of science and research and its application in real life scenarios is maybe the main defining characteristic of the work. The framework is not a purely scientific result, intended for laboratory experiments. It lives from the constant interaction with actual organizations and their objectives and requirements. On the other side, it is not simply a predefined framework that an organisation can apply as it is. It needs to be more or less tailored to organizations objectives and requirements. This requires an in depth understanding of the organization as well as the elements of the framework.

9.5 Potentials for future applications and further development

The modular structure of the framework and its generic nature makes it a good starting point for future applications and further development.

After the clarification of the ISMS core process framework supporting the operation of an ISMS the processes must be performed by persons. For this roles must be defined and assigned to the steps of the ISMS core processes. The comprehension of roles, accountabilities and responsibilities in all processes is a key success factor for an effective and efficient management. An established method to define who is doing what in within a process is the RACI-model. Thus, an opportunity for further development is the definition of RACI charts for every process of the framework.

According to Mayer and Fagundes (2009) also a method for identifying process specific control objectives per maturity level is of interest for further research. This would support the management of the processes.

9.6 Outlook on future research activities

Based on the potentials of the framework and the state-of-the-art research in the relevant areas the following lines of future research can be envisioned.

1) Further pilot application in different sectors and organization of different sizes would build a basis for the further optimization of the framework. This would also clear the way for sector or size specific adaptions of the framework.
2) Further studies should be conducted to reach a consensus regarding the elements of the process descriptions within the community of interest (see also ISO/IEC 33004 chapter 5.3.2)
3) Enhancement of the framework by including the definition of RACI charts for every process of the framework as well as process specific control objectives per maturity level.
4) Research regarding an integrated process framework of information security management, (IT-) service management, data protection management as well as the overall risk management and business continuity management could result in an integrated and generic state of the art process framework.
5) As no resilient information about the actual usage of maturity level models within ISMS are available, this should be investigated in further research.
6) Based on further applications the effects of and the method to determine the necessary process maturity level itself should be investigated in further research regarding:
    a) identification of optimization potentials
    b) scientific analysis of the effects of the method.

10 References

Aceituno, V. (2007). ISM3-Information Security Managemente Maturity Model v. 2.1. *ISM3 Consortium*.

Alexander, R. D., & Panguluri, S. (2017). Cybersecurity Terminology and Frameworks. In *Cyber-Physical Security* (pp. 19–47). Springer.

Alpar, P., Alt, R., Bensberg, F., Grob, H. L., Weimann, P., & Winter, R. (2016). Phasenmodelle in der Systementwicklung. In *Anwendungsorientierte Wirtschaftsinformatik* (pp. 331–374). Springer.

Alvaro, A. (2009). Sicherheit in der Informationsgesellschaft. In *Freiheit: gefühlt–gedacht–gelebt* (pp. 214–227). Springer.

Anam, S., Kim, Y. S., Kang, B. H., & Liu, Q. (2016). Adapting a knowledge-based schema matching system for ontology mapping. In *Proceedings of the Australasian Computer Science Week Multiconference* (p. 27). ACM.

Anderson, K.-U. (2014). From Here to Maturity - Managing the Information Security Life Cycle. *ISACA Journal*, *6*, 8.

Asma'Mokhtar, U., Yusof, Z. M., Ahmad, K., & Jambari, D. I. (2016). Development of function-based classification model for electronic records. *International Journal of Information Management*, *36*(4), 626–634.

Baldassarre, M. T. (2016). A 360-degree process improvement approach based on multiple models. *Revista de La Facultad de Ingeniería*, *30*(4).

Baldassarre, M. T., Caivano, D., Pino, F. J., Piattini, M., & Visaggio, G. (2012). Harmonization of ISO/IEC 9001: 2000 and CMMI-DEV: from a theoretical comparison to a real case application. *Software Quality Journal*, *20*(2), 309–335.

Barafort, B., Mesquida, A.-L., & Mas, A. (2016). How to Integrate Risk Management in IT Settings Within Management Systems? Comparison and Integration Perspectives from ISO Standards. In *International Conference on Software Process Improvement and Capability Determination* (pp. 254–269). Springer.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, *51*(1), 138–151.

Becker, J., & Kahn, D. (2003). The process in focus. In *Process management* (pp. 1–12). Springer.

Benner, M. J., & Tushman, M. (2002). Process management and technological innovation: A longitudinal study of the photography and paint industries. *Administrative Science Quarterly*, *47*(4), 676–707.

Benner, M. J., & Tushman, M. L. (2003). Exploitation, exploration, and process management: The productivity dilemma revisited. *Academy of Management Review*, *28*(2), 238–256.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM*, *48*(2), 78–83.

Boehmer, W. (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. *SECURWARE*, *8*, 224–231.

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: a state-of-the-art assessment. *MIS Quarterly*, 1–16.

Bowen, P., & Kissel, R. (2007a). *Program Review for Information Security Management Assistance (PRISMA)*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Bowen, P., & Kissel, R. (2007b). *Program Review for Information Security Management Assistance (PRISMA)*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Brenner, J. (2007). ISO 27001: Risk management and compliance. *RISK MANAGEMENT-NEW YORK-*, *54*(1), 24.

BSI UK. (2013). *Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013*. Milton Keynes.

Buecker, A., Borrett, M., Lorenz, C., & Powers, C. (2010). Introducing the IBM security framework and IBM security blueprint to realize business-driven security. *Redguides for Business Leaders REDP-4528-01*.

Buglione, L., & Abran, A. (2006). Introducing root-cause analysis and orthogonal defect classification at lower CMMI maturity levels. *Proc. MENSURA*, 29.

Calder, A. (2009). *Information Security Based on ISO 27001/ISO 27002: A Management Guide*. Van Haren Publishing.

Calder, A., & Watkins, S. G. (2010). *Information security risk management for ISO27001/ISO27002*. It Governance Ltd.

Calvo-Manzano, J. A., Cueva, G., & Muñoz, M. (2008). Project Management Similarity Study: Experiment on Project Planning Practices Based on CMMI-Dev v1.2. In *EuroSPI 2008 - Proceedings* (p. 11). Dublin: PUBLIZON.

Canal, V. A. (2008). Usefulness of an Information Security Management Maturity Model. *Information System Control Journal*, *2*.

Canal, V. A. (n.d.). ISM3 1.0. *Information Security Management Maturity Model*.

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A Framework for Information Security Governance and Management. *IT Professional*, *18*(2), 22–30.

Chang, S.-I. (2005). An alternative methodology for Delphi-type research in IS key issues studies. *International Journal of Management and Enterprise Development*, *3*(1–2), 147–168.

Chaudhary, M., & Chopra, A. (2017). CMMI for development: implementation guide.

Cholez, H., & Girard, F. (2014). Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of Software: Evolution and Process*, *26*(5), 496–503.

CMMI Product Team. (2010a). Capability Maturity Model Integration for Acquisition, Version 1.3 (CMU/SEI-2010-TR-032. *Software Engineering Institute, Carnegie Mellon University*.

CMMI Product Team. (2010b). Capability Maturity Model Integration for Development, Version 1.3 (CMU/SEI-2010-TR-033). *Software Engineering Institute, Carnegie Mellon University*.

CMMI Product Team. (2010c). Capability Maturity Model Integration for Services, Version 1.3 (CMU/SEI-2010-TR-034). *Software Engineering Institute, Carnegie Mellon University*.

Coelho, R. W., Fernandes Jr, G., & Proença Jr, M. L. (2014). GAIA-MLIS: A Maturity Model for Information Security. *SECURWARE 2014*, 61.

Cots, S., Casadesús, M., & Marimon, F. (2016). Benefits of ISO 20000 IT service management certification. *Information Systems and E-Business Management*, *14*(1), 1–18.

Coulson, T., Zhu, J., Miyuan, S., & Rohm, T. (2015). The price of security: the challenge of measuring business value investments in securing information systems. *Communications of the IIMA*, *5*(4), 3.

Delgado, A. P., & Velthuis, M. P. (2014). Current state of IT Governance in banking. In *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1–6). IEEE.

Dombora, S. (2016). Characteristics of Information Security Implementation Methods. *Volume of Management, Enterprise and Benchmarking in the 21st Century III*, 57–72.

Donnelly, J. P. (2017). A systematic review of concept mapping dissertations. *Evaluation and Program Planning*, *60*, 186–193.

Drescher, M., Perera, A., Johnson, C., Buse, L., Drew, C., & Burgman, M. (2013). Toward rigorous use of expert knowledge in ecological research. *Ecosphere*, *4*(7), art83.

Drljača, D., & Latinović, B. (2017). Frameworks for Audit of an Information System in Practice. *JITA-JOURNAL OF INFORMATION TECHNOLOGY AND APPLICATIONS*, *12*(2).

Dubé, L., & Paré, G. (2003). Rigor in information systems positivist case research: current practices, trends, and recommendations. *MIS Quarterly*, 597–636.

Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A systematic approach to define the domain of information system security risk management. In

Intentional Perspectives on Information Systems Engineering (pp. 289–306). Springer.

Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly*, *26*(4), 584–593.

Eloff, J., & Eloff, M. (2005). Information security architecture. *Computer Fraud & Security*, *2005*(11), 10–16.

Eloff, J. H., & Eloff, M. (2003). Information security management: a new paradigm. In *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology* (pp. 130–136). South African Institute for Computer Scientists and Information Technologists.

Ernerot, H., & Torstensson, F. (2017). *Harmoni mellan verksamhet och IT: En litteraturstudie*.

Eshlaghy, A. T., Pourebrahimi, A., & Nobari, B. Z. (2011). Presenting a Model for Ranking Organizations Based on the Level of the Information Security Maturity. *Computer and Information Science*, *4*(1), 72.

Fakhri, B., Fahimah, N., & Ibrahim, J. (2015). Information Security Aligned To Enterprise Management. *Middle East Journal of Business*, *10*(1).

Fenz, S., & Ekelhart, A. (2009). Formalizing information security knowledge. In *Proceedings of the 4th international Symposium on information, Computer, and Communications Security* (pp. 183–194). ACM.

Frank, T. (2016). Towards a document-driven approach for designing reference models: From a conceptual process model to its application. *Journal of Systems and Software*, *111*, 254–269.

García-Mireles, G. A., Moraga, M. Á., & García, F. (2012). Development of maturity models: a systematic literature review. In *Evaluation & Assessment in Software Engineering (EASE 2012), 16th International Conference on* (pp. 279–283). IET.

Gentner, D. (1983). Structure-mapping: A theoretical framework for analogy. *Cognitive Science*, *7*(2), 155–170.

German Federal Office for Information Security. (2008). *BSI-Standard 100-1*. Bonn.

German Federal Office for Information Security. (2013). *IT-Grundschutz Catalogues* (13th ed.). Bonn.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438–457.

Gordon, L. A., & Loeb, M. P. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, *49*(1), 121–125.

Gottschalk, P., & Solli-Sæther, H. (2006). Maturity model for IT outsourcing relationships. *Industrial Management & Data Systems*, *106*(2), 200–212.

Guo, W., & Kraines, S. B. (2008). Explicit scientific knowledge comparison based on semantic description matching. *Proceedings of the American Society for Information Science and Technology*, *45*(1), 1–18.

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). Security Management Standards: A mapping. Presented at the Conference on

ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist, Porto, Portugal.

Hevner, A., & Chatterjee, S. (2010). *Design research in information systems: theory and practice* (Vol. 22). Springer Science & Business Media.

Howard, J. D., & Longstaff, T. A. (1998). A common language for computer security incidents. *Sandia National Laboratories*.

Huang, S.-J., & Han, W.-M. (2008). Exploring the relationship between software project duration and risk exposure: A cluster analysis. *Information & Management*, *45*(3), 175–182.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255.

Hwang, S. M. (2009). Process quality levels of ISO/IEC 15504, CMMI and K-model. *International Journal of Software Engineering and Its Applications*, *3*(1), 33–42.

Information Systems Audit and Control Association. (2008). *IT-Governance and Process Maturity*. Rolling Meadows.

Information Systems Audit and Control Association. (2009). *An Introduction to the Business Model for Information Security*. Rolling Meadows.

Information Systems Audit and Control Association. (n.d.-a). *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows.

Information Systems Audit and Control Association. (n.d.-b). *COBIT 5 Enabling Processes*. Rolling Meadows.

Information Systems Audit and Control Association. (n.d.-c). *COBIT 5 for Information Security*. Rolling Meadows.

Information Systems Audit and Control Association. (n.d.-d). *COBIT 5 Process Assessment Model (PAM): Using COBIT 5*. Rolling Meadows.

Information Systems Audit and Control Association. (n.d.-e). *Self-assessment Guide Using COBIT 5*. Rolling Meadows.

International Organization for Standardization. (2011). *ISO/IEC 19011:2011*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2003). *ISO/IEC 15504-2:2003*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2004a). *ISO/IEC 15504-1:2004*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2004b). *ISO/IEC 15504-3:2004*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2005). *ISO 9000:2005*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2008). *ISO/IEC 15504-4:2008*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2009). *ISO/IEC 21827:2008*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2010). *ISO/IEC 27003:2010*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2010). *ISO/IEC 27004:2010*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2010). *ISO/IEC/TR 24774*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2011). *ISO/IEC 20000-1:2011*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2011). *ISO/IEC 27005:2011*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2011). *ISO/IEC 27006:2011*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2012a). *ISO/IEC 15504-5:2012*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2012b). *ISO/IEC 20000-2:2012*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2013). *ISO/IEC 15504-6:2013*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2013). *ISO/IEC 27001:2013*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2013). *ISO/IEC 27002:2013*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (2014). *ISO/IEC 27000:2014*. Geneva.

International Organization for Standardization and International Electrotechnical Commission. (n.d.). *ISO/IEC 27000 series*. Geneva.

ISO/IEC 21827:2008. (2008). Geneva.

ISO/IEC 33004:2015. (2015). Geneva.

ISO/IEC 33020:2015. (2015a). Geneva.

ISO/IEC 38500:2015. (2015b). Geneva.

Jalali, S., & Wohlin, C. (2012). Systematic literature studies: database searches vs. backward snowballing. In *Proceedings of the ACM-IEEE international symposium on Empirical software engineering and measurement* (pp. 29–38). ACM.

Javidan, M. (1998). Core competence: what does it mean in practice? *Long Range Planning*, *31*(1), 60–71.

Jeston, J., & Nelis, J. (2014). *Business Process Management*. Routledge.

Karokola, G., Kowalski, S., & Yngström, L. (2011). Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View. In *HAISA* (pp. 58–73).

Kasulke, S., & Bensch, J. (2017). ISO, ITIL & Co.–Basis und Orientierung schaffen. In *Zero Outage* (pp. 15–24). Springer.

Kautz, K., Madsen, S., & Nørbjerg, J. (2007). Persistent problems and practices in information systems development. *Information Systems Journal*, *17*(3), 217–239.

Keele, S. (2007). Guidelines for performing systematic literature reviews in software engineering. In *Technical report, Ver. 2.3 EBSE Technical Report. EBSE*.

Kirinic, V., & Kozina, M. (2016). Maturity Assessment of Strategy Implementation in Higher Education Institution. In *Central European Conference on Information and Intelligent Systems* (p. 169). Faculty of Organization and Informatics Varazdin.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, *33*(2004), 1–26.

Kitchenham, B. A., Budgen, D., & Brereton, O. P. (2011). Using mapping studies as the basis for further research–a participant-observer case study. *Information and Software Technology*, *53*(6), 638–651.

Kittel, M., Koerting, T. J., & Schött, D. (2006). *Kompendium für ITIL-Projekte*. readIT.

Krabbes, K. (2016). Die Zertifizierung in der Informationssicherheit. In *Zertifizierung als Erfolgsfaktor* (pp. 539–550). Springer.

Laita, A., & Belaissaoui, M. (2017). Information Technology Governance in Public Sector Organizations. In *Europe and MENA Cooperation Advances in Information and Communication Technologies* (pp. 331–340). Springer.

Larrucea, X., Santamaría, I., & Colomo-Palacios, R. (2016). Assessing ISO/IEC29110 by means of ITMark: results from an experience factory. *Journal of Software: Evolution and Process*, *28*(11), 969–980.

Lasrado, L. A., Vatrapu, R., & Andersen, K. N. (2015). Maturity Models Development in IS Research: A Literature Review.

Leopold, H., Pittke, F., & Mendling, J. (2013). Towards Measuring Process Model Granularity via Natural Language Analysis. In *4th International Workshop on Process Model Collections: Management and Reuse (PMC-MR 2013), Beijing, China*.

Lessing, M. (2008). Best practices show the way to Information Security Maturity.

Lincoln, Y. S., Lynham, S. A., & Guba, E. G. (2011). Paradigmatic controversies, contradictions, and emerging confluences, revisited. *The Sage Handbook of Qualitative Research*, *4*, 97–128.

Lindström, J., Samuelsson, S., Harnesk, D., & Hägerfors, A. (2008). The need for improved alignment between actability, strategic planning of IS and information security. In *Conference Proceedings of the 13th International ITA Workshop, Krakow, Poland* (pp. 4–6).

Luftman, J. (2000). Assessing business-IT alignment maturity. *Communications of the AIS, 4,* 1–50.

Mangin, O., Barafort, B., Heymans, P., & Dubois, E. (2012). Designing a process reference model for information security management systems. In *Software Process Improvement and Capability Determination* (pp. 129–140). Springer.

Martins, A., & Elofe, J. (2002). *Information security culture*. Springer.

Masinsin, L. C. R. Q., & Corps, U. M. (2008). Secretary of Defense Corporate Fellows Program.

Matrane, O., & Talea, M. (2014). A Maturity Model for Information Security Management in Small and Medium-Sized Moroccan Enterprises: An Empirical Investigation. *International Journal of Advanced Research in Computer Science*, *5*(6).

Mayer, J., & Fagundes, L. L. (2009). A model to assess the maturity level of the risk management process in information security. In *Integrated Network Management-Workshops, 2009. IM'09. IFIP/IEEE International Symposium on* (pp. 61–70). IEEE.

Mehairjan, R. P. Y. (2017). Asset, Risk and Maintenance Management. In *Risk-Based Maintenance for Electricity Network Organizations* (pp. 9–30). Springer.

Meroth, A. M., Trankle, F., Richter, B. F., Wagner, M., Neher, M., & Luling, J. (2015). Functional safety and development process capability for intelligent

transportation systems. *IEEE Intelligent Transportation Systems Magazine*, *7*(4), 12–23.

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational Characteristics Influencing SME Information Security Maturity. *Journal of Computer Information Systems*, *56*(2), 106–115.

Miloslavskaya, N., & Sagirov, R. (2016). Review of Information Security Processes' Maturity Models.

Mitasiunas, A., Novickis, L., & Kalpokas, R. (2014). Security Process Capability Model Based on ISO/IEC 15504 Conformant Enterprise SPICE. *Applied Computer Systems*, *15*(1), 36–41.

Mohamed, S. F. P., Baharom, F., Deraman, A., Yahya, J., & Mohd, H. (2016). An Exploratory Study on Secure Software Practices Among Software Practitioners in Malaysia. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *8*(8), 39–45.

Murine, G., & Carpenter, J. C. (1984). Measuring computer system security using software security metrics. In *Proceedings of the 2nd IFIP international conference on Computer security: a global challenge* (pp. 207–215). North-Holland Publishing Co.

Myers, M. D., & others. (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, *21*(2), 241–242.

Narayanan, M. (2010). Information Security Management Systems (ISMS) – A comparison between ISO 27001 and ISM3. Retrieved from http://www.anupnarayanan.org/ism3andiso27001.pdf

Neap, H. S., & Celik, T. (1999). Value of a product: A definition. *International Journal of Value-Based Management*, *12*(2), 181–191.

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

Nofer, D.-K. 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.

Nolan, R. L. (1973). Managing the computer resource: a stage hypothesis. *Communications of the ACM*, *16*(7), 399–405.

Norman, A. A., & Yasin, N. M. (2013). Information Systems Security Management (ISSM) Maturity Factors In E-Commerce Malaysia. *Australian Journal of Basic and Applied Sciences*, *7*(9), 165–173.

Oates, B. J. (2005). *Researching information systems and computing*. Sage.

Office of Government Commerce. (2007a). *ITIL v3 Service Design*. London.

Office of Government Commerce. (2007b). *ITIL v3 Service Improvement*. London.

Office of Government Commerce. (2007c). *ITIL v3 Service Lifecycle*. London.

Office of Government Commerce. (2007d). *ITIL v3 Service Operation*. London.

Office of Government Commerce. (2007e). *ITIL v3 Service Strategy*. London.

Office of Government Commerce. (2007f). *ITIL v3 Service Transition*. London.

Ormrod, D., & Turnbull, B. (2016). The Military Cyber-Maturity Model: Preparing Modern Cyber-Enabled Military Forces for Future Conflicts. In *11th International Conference on Cyber Warfare and Security: ICCWS2016* (p. 261). Academic Conferences and publishing limited.

Pardo, C., Pino, F. J., García, F., Piattini, M., & Baldassarre, M. T. (2010). A process for driving the harmonization of models. In *Proceedings of the 11th International Conference on Product Focused Software* (pp. 51–54). ACM.

Pare, G., Cameron, A.-F., Poba-Nzaou, P., & Templier, M. (2013). A systematic assessment of rigor in information systems ranking-type Delphi studies. *Information & Management*, *50*(5), 207–217.

Paulk, M. C. (1993). Comparing ISO 9001 and the capability maturity model for software. *Software Quality Journal*, *2*(4), 245–256.

Peltier, T. R. (2013). *Information security fundamentals*. CRC Press.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC Press.

Phillips, M. (2003a). Using a Capability Maturity Model to Derive Security Requirements. Retrieved from http://www.sans.org/reading-room/whitepapers/bestprac/capability-maturity-model-derive-security-requirements-1005

Phillips, M. (2003b). Using a capability maturity model to derive security requirements. *SANS InfoSec Reading Room, GSEC Practical v1*.

Pieters, W., Probst, C. W., Lukszo, S., & Montoya, L. (2014). Cost-effectiveness of Security Measures: A model-based Framework. *Approaches and Processes for Managing the Economics of Information Systems*, 139.

Poepjes, R. (2015). *The development and evaluation of an information security awareness capability model: linking ISO/IEC 27002 controls with awareness importance, capability and risk*. University of Southern Queensland.

Poeppelbuss, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity models in information systems research: literature search and analysis. *Communications of the Association for Information Systems*, *29*(27), 505–532.

Predoiu, L., Feier, C., Scharffe, F., Bruijn, J. de, Martín-Recuerda, F., Manov, D., & others. (2005). *State-of-theart survey on ontology merging and aligning. Digital Research Institute, University of Innsbruck*.

Publishing, V. H. (2007). *IT service management: an introduction*. Van Haren Publishing.

Qureshi, N., Usman, M., & Ikram, N. (2013). Evidence in software architecture, a systematic literature review. In *Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering* (pp. 97–106). ACM.

Ramar, K., & Gurunathan, G. (2016). Technical Review on Ontology Mapping Techniques. *Asian Journal of Information Technology*, *15*(4), 676–688.

Rao, V., & Jamieson, R. (2003). An Approach to Implementing Maturity Models in IT Security. *ACIS 2003 Proceedings*, 25.

Ridley, G., Young, J., & Carroll, P. (2004). COBIT and its Utilization: A framework from the literature. In *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on* (p. 8–pp). IEEE.

Saeed, K. A., & Abdinnour, S. (2013). Understanding post-adoption IS usage stages: an empirical assessment of self-service information systems. *Information Systems Journal*, *23*(3), 219–244.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In

Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on (pp. 749–753). IEEE.

Saint-Germain, R., & others. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal*, *39*(4), 60–66.

Saleh, M. F. (2011). Information security maturity model. *International Journal of Computer Science and Security (IJCSS)*, *5*(3), 21.

Salviano, C. F., & Figueiredo, A. M. C. (2008). Unified Basic Concepts for Process Capability Models. In *SEKE* (pp. 173–178).

Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. *MIS Quarterly*, 237–263.

Sanchez, L. E., Villafranca, D., & Piattini, M. (2007). MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. In *WOSIS* (pp. 233–244).

Sanchez-Gordón, M.-L., Colomo-Palacios, R., & Herranz, E. (2016). Gamification and Human Factors in Quality Management Systems: Mapping from Octalysis Framework to ISO 10018. In *European Conference on Software Process Improvement* (pp. 234–241). Springer.

Santos, G., Rebelo, M., & Silva, R. (2017). The integration of standardized Management Systems: managing Business Risk. *International Journal of Quality & Reliability Management*, *34*(3).

Scheer, A.-W., & Nüttgens, M. (2000). *ARIS architecture and reference models for business process management*. Springer.

Scholderer, R. (2016). *Management von Service-Level-Agreements: methodische Grundlagen und Praxislösungen mit CobiT, ISO 20000 und ITIL*. dpunkt. verlag.

Schwickert, P. P. D. A. C., & others. (2017). Projekt: Control-Framework für IT-Compliance im Kontext der Corporate Governance.

Shanteau, J. (1992). Competence in experts: The role of task characteristics. *Organizational Behavior and Human Decision Processes*, *53*(2), 252–266.

Siponen, M. (2002). Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria. *Information Management & Computer Security*, *10*(5), 210–224.

Siponen, M. (2006a). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), 97–100.

Siponen, M. (2006b). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), 97–100.

Slack, N., Chambers, S., & Johnston, R. (2010). *Operations management*. Pearson Education.

Slot, G. (2015). Towards Rule-based Information Security Maturity.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225.

Sowa, A. (2017a). Management der Informationssicherheit als Prozess. In *Management der Informationssicherheit* (pp. 17–33). Springer.

Sowa, A. (2017b). Management der Informationssicherheit als Prozess. In *Management der Informationssicherheit* (pp. 17–33). Springer.

Spósito, M. A. F., Neto, A. C. D., & da Silva Barreto, R. (2016). Business-IT Alignment Research Field.

Stacey, T. R. (1996). Information security program maturity grid. *Information Systems Security*, *5*(2), 22–33.

Stambul, M. A. M., & Razali, R. (2011). An assessment model of information security implementation levels. In *Electrical Engineering and Informatics (ICEEI), 2011 International Conference on* (pp. 1–6). IEEE.

Steiner, W. (n.d.). Ein Zielsystem im Unternehmen: So implementieren Sie es richtig. *IT-GOVERNANCE*, *9*(21), 14–19.

Stevanović, B. (2011). Maturity models in information security. *International Journal of Information*, *1*(2).

Stevanović, B. (2011). Maturity Models in Information Security. *International Journal of Information*, *1*(2).

Stevanović, B. (2011). Maturity models in information security. *International Journal of Information*, *1*(2).

Stoll, M. (2014). An Information Security Model for Implementing the New ISO 27001. *Handbook of Research on Emerging Developments in Data Privacy*, 216.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 147–169.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), 23–29.

Suwito, M. H., Matsumoto, S., Kawamoto, J., Gollmann, D., & Sakurai, K. (2016). An Analysis of IT Assessment Security Maturity in Higher Education Institution. In *Information Science and Applications (ICISA) 2016* (pp. 701–713). Springer.

Tarhan, A., Turetken, O., & Reijers, H. A. (2016). Business process maturity models: a systematic literature review. *Information and Software Technology*, *75*, 122–134.

The Open Group. (2011). *Open Information Security Management Maturity Model (O-ISM3)*. Berkshire: The Open Group.

The Open Group. (2014). *Optimizing ISO/IEC 27001:2013 using O-ISM3*. Berkshire: The Open Group.

The Open Group | The Open Group Releases Maturity Model for Information Security Management. (n.d.). Retrieved July 4, 2014, from http://www.opengroup.org/news/press/open-group-releases-maturity-model-information-security-management

Turner, M. (2010). Digital libraries and search engines for software engineering research: An overview. *Keele University, UK*.

U.S. Department of Commerce - National Institute of Standards and Technology. (n.d.). *NIST Special Publication 800 series*. Gaithersburg.

Uskarcı, A., & Demirörs, O. (2017). Do staged maturity models result in organization-wide continuous process improvement? Insight from employees. *Computer Standards & Interfaces*, *52*, 25–40.

Van Steenbergen, M., Bos, R., Brinkkemper, S., Van De Weerd, I., & Bekkers, W. (2010). The design of focus area maturity models. In *Global Perspectives on Design Science Research* (pp. 317–332). Springer.

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. *Information Systems Management*, *24*(4), 361–372.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*(1), 21–54.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, *24*(2), 99–104.

von Wangenheim, C. G., Hauck, J. C. R., Salviano, C. F., & von Wangenheim, A. (2010). Systematic literature review of software process capability/maturity models. In *INTERNATIONAL CONFERENCE ON SOFTWARE PROCESS IMPROVEMENT AND CAPABILITY DETERMINIATION–SPICE*.

Vuppala, V., Vincent, J., Kusler, J., & Davidson, K. (2011.). Securing a Control System: Experiences from ISO 27001 Implementation. *Proceedings of ICALEPCS2011, Grenoble, France*.

Wester, K. L. (2011). Publishing Ethical Research: A Step-by-Step Overview. *Journal of Counseling & Development*, *89*(3), 301–307.

Whitman, M., & Mattord, H. (2013). *Management of information security*. Cengage Learning.

Woodhouse, S. (2008). An isms (im)-maturity capability model. In *Computer and Information Technology Workshops, 2008. CIT Workshops 2008. IEEE 8th International Conference on* (pp. 242–247). IEEE.

Worrell, J. L., Di Gangi, P. M., & Bush, A. A. (2013). Exploring the use of the Delphi method in accounting information systems research. *International Journal of Accounting Information Systems*, *14*(3), 193–208.

Xiao-yan, G., Yu-qing, Y., & Li-lei, L. (2011a). An information security maturity evaluation mode. *Procedia Engineering*, *24*, 335–339.

Xiao-yan, G., Yu-qing, Y., & Li-lei, L. (2011b). An information security maturity evaluation mode. *Procedia Engineering*, *24*, 335–339.

Yeh, K. B., Adams, M. L., Marshall, E. S., Dasgupta, D., Zhunushov, A., Richards, A. L., & Hay, J. (2017). Applying a Capability Maturity Model (CMM) to evaluate global health security-related research programmes in under-resourced areas. *Global Security: Health, Science and Policy*, *2*(1), 1–9.

11 Appendix A – Publications

Likewise, and in the regard to this thesis, the PhD student has published and presented the following papers to an international audience:

- Journal papers with impact factor
  - Knud Brandis, Srdan Dzombeta, and Knut Haufe. **"Towards a framework for governance architecture management in cloud environments: A semantic perspective."** Future Generation Computer Systems 32 (2014): 274-281 – Impact factor 2014: 2.786; COMPUTER SCIENCE, THEORY & METHODS, 8/102, Q1) http://dx.doi.org/10.1016/j.future.2013.09.022
  - Dzombeta, S., Stantchev, V., Colomo-Palacios, R., Brandis, K., & Haufe, K. (2014). **Governance of cloud computing services for the life sciences – the case of Germany in the context of EU**. IEEE IT Professional, 16(4), 30-37. (Impact factor 2014: 0.819; COMPUTER SCIENCE, INFORMATION SYSTEMS, 62/104, Q3) http://dx.doi.org/10.1109/MITP.2014.52
  - Knut Haufe, Srdan Dzombeta, Knud Brandis, Vladimir Stantchev and Ricardo Colomo-Palacios. **"The growing relevance of cost governance in it security management"** – accepted in IT Professional - publication pending (Impact factor 2015: 1.067; COMPUTER SCIENCE, SOFTWARE ENGINEERING, 47/106, Q2)
- Journal papers without impact factor
  - Knut Haufe, Ricardo Colomo-Palacios, Srdan Dzombeta, Knud Brandis and Vladimir Stantchev. **"A process framework for information security management"** - International Journal of Information Systems and Project Management – 2016, 27-47, Vol. 4, No. 4
  - Knut Haufe, Srdan Dzombeta, and Knud Brandis. **"Proposal for a Security Management in Cloud Computing for Health Care."** The Scientific World Journal 2014 (2014) – http://dx.doi.org/10.1155/2014/146970
- Conferences
  - Knut Haufe, Ricardo Colomo-Palacios, Srdan Dzombeta, Knud Brandis and Vladimir Stantchev. "**ISMS core processes: A study**" – Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016, Volume 100, pp. 339-346, Porto, Portugal, October 5-7, 2016 http://dx.doi.org/10.1016/j.procs.2016.09.167
  - Knut Haufe, Ricardo Colomo-Palacios, Srdan Dzombeta, Knud Brandis and Vladimir Stantchev. "**Security Management Standards: A mapping**" – Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016, Volume 100,

pp. 755-761, Porto, Portugal, October 5-7, 2016 http://dx.doi.org/10.1016/j.procs.2016.09.221

- Other papers or books
  - Audit Guideline for commissioned data processing, ISACA Germany Chapter e.V. (ed.) 2011 (together with Dr. Aleksandra Sowa, Christian Funk, Michael Trinkle, Michael Morgenthaler, Claus Baumgarten, Andreas H. Schmidt, Michael Neuy)
  - Applying ISO 31000 in IT, ISACA Germany Chapter e.V. (ed.) Published in 2015 (together with other authors)
  - Modules “Windows Server 2003” and “Windows 7” for the IT-Grundschutz catalogues (co-author), Federal Office for Information Security
  - Operation and optimization of management systems for information security (ISMS) with the use of DIN ISO/IEC 27001 - ISBN-13: 978-3410260325, Beuth Verlag, 2017

12 Appendix B – Process Profiles

In the following detailed process profiles as well as process charts are documented.

As every ISMS process provides input for the documentation and records control process and the ISMS planning process provides input for every ISMS process those interfaces are generally not displayed in the process charts to enable a better readability.

Process profiles are oriented on ITIL process documentation template – appendix c from Service Design (Office of Government Commerce, 2007a, p. 249)

12.1 ISMS planning process

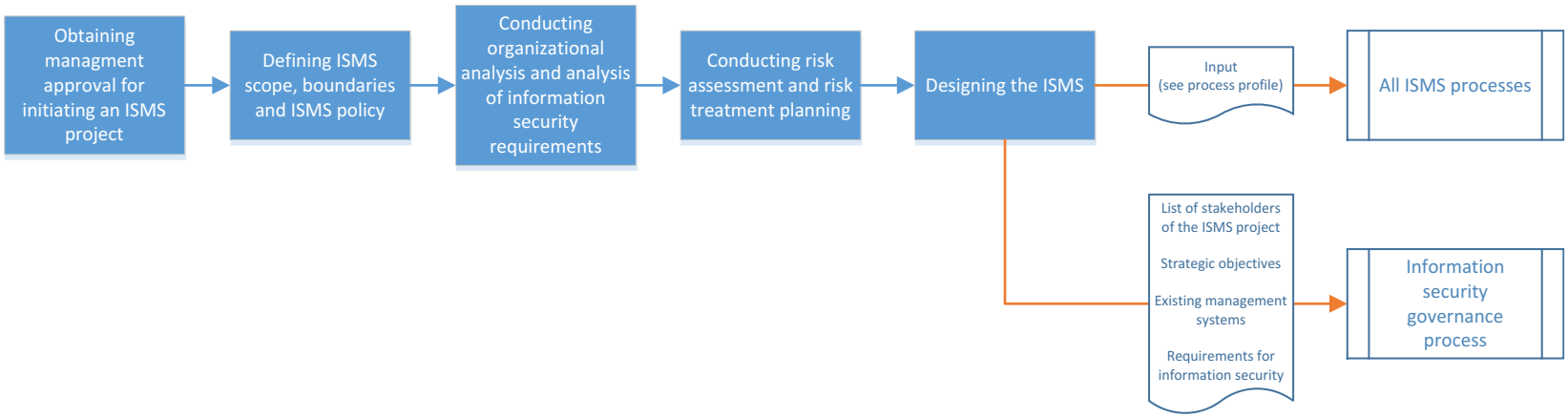

Figure 19 – ISMS planning process chart

Process name	ISMS planning process (derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a))
Process category	Management process
Brief description	The ISMS planning process is the process of ISMS specification and design from inception to the production of implementation plans.
Objectives/purposes	• Start the ISMS project • Defined scope/boundaries of the ISMS and ISMS policy • Endorsement of the management for the ISMS • Defined relevant requirements • Initial identification of information assets and their current security status • Defined risk assessment methodology and initially identified, analyzed and evaluated security risks as well as selected treatment options and control objectives for controls • Complete the final ISMS implementation plan
Input	• None
Output	• For information security governance process: – List of stakeholders of the ISMS project – Strategic objectives – Existing management systems – Requirements for information security • Provides input for all ISMS processes: – Objectives, priorities and organizational requirements for the ISMS – Applicable information security requirements and assets – Outlined characteristics of the business, the organization, its location, assets and technology – Management approval for initiating the ISMS – Documented business case for the ISMS / Project proposal – ISMS scope and boundaries – ISMS policy – Results from information security assessment – Description of risk assessment methodology – Results of risk assessment and risk treatment plan – Management acceptance of residual risks – List of control objectives and selected controls – ISMS project implementation plan including roles, responsibilities and necessary resources – Organization structure, roles and responsibilities for information security – A document summarizing the requirements for ISMS records and documentation control – Repositories and templates for ISMS records – Information security standards and procedures – Management review plan including management

Process name	ISMS planning process (derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a))
	review procedures (auditing and monitoring and measuring aspects) – Defined information security training team and information security awareness, education and training materials, pans, and records
Activities/functions	• Obtaining management approval for initiating an ISMS project • Defining ISMS scope, boundaries and ISMS policy • Conducting organizational analysis and analysis of information security requirements • Conducting risk assessment and risk treatment planning • Designing the ISMS
Metrics	Effectiveness and efficiency of every ISMS process integrated into an information security measurement program
Owner	Top Management
Manager	Information security officer
Actors	Information security committee and planning team Specialists Consultants Asset owners like line managers or process owners Legal advisors Risk manager

Table 55 – Process profile ISMS planning process

12.2 Information security risk assessment process

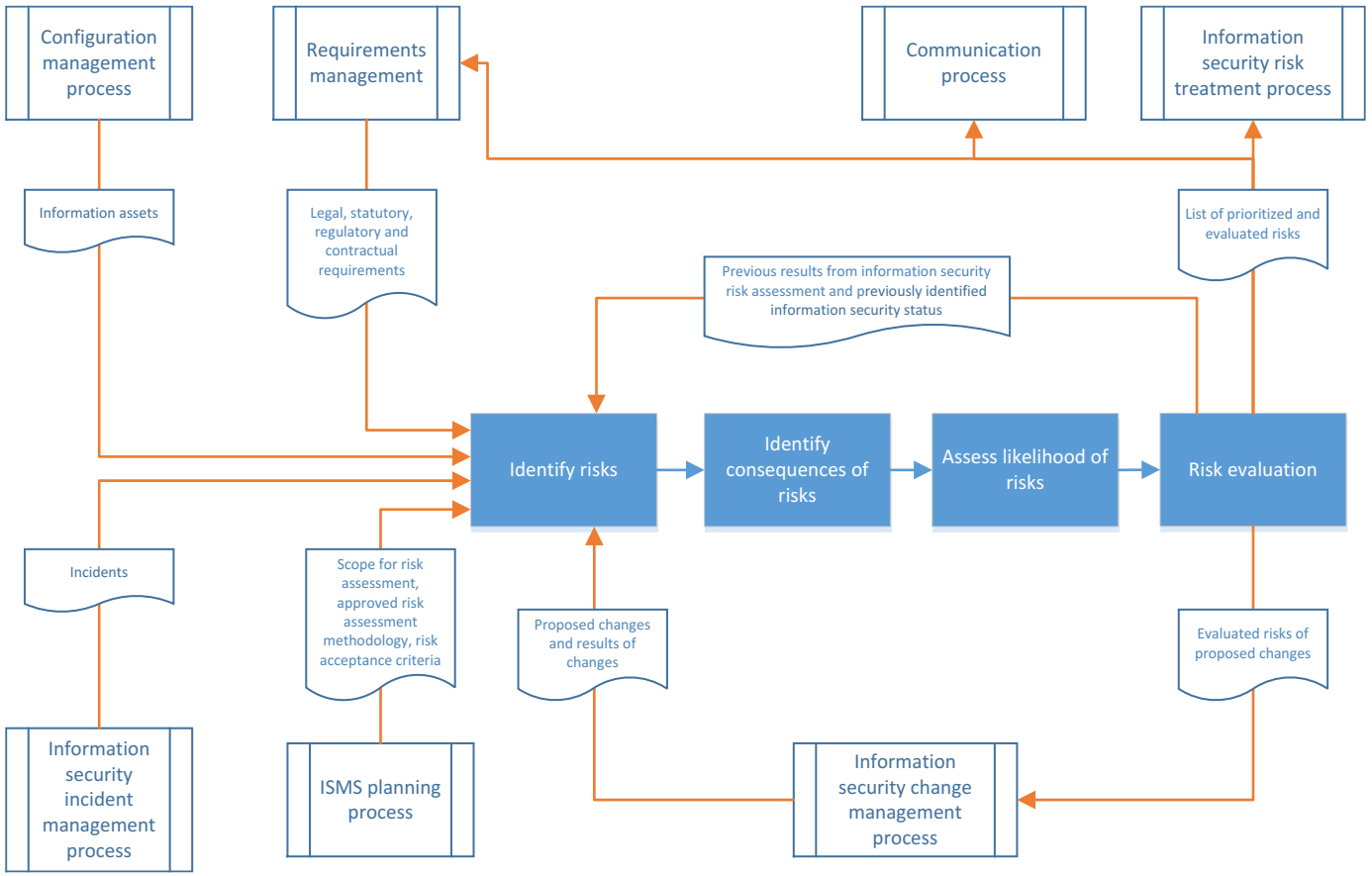

Figure 20 – Information security risk assessment process chart

Process name	**Information security risk assessment process – derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2011)**
Process category	ISMS core process
Brief description	The information security risk assessment process is the overall process of risk identification, analysis and risk evaluation.
Objectives/purposes	• Identify, analyze and evaluate information security risks • Consistent, valid and comparable results of risk assessment • Identify risk owners
Input	• From ISMS planning process (ISMS scope and policy): – Scope for risk assessment – Approved risk assessment methodology – Risk acceptance criteria • From information security risk assessment process itself: – Previous results from information security risk assessment – Previously identified information security status • From configuration management process: information assets • From requirements managements: legal, statutory, regulatory and contractual requirements • From information security change management process: proposed changes and results of changes • From information security incident management process: incidents
Output	• To information security risk treatment process, communication and requirements management process: documented and evaluated risks in a list of prioritized risks including – Threats, vulnerabilities and risk owners – consequences and business impact, – likelihood and comparison against risk criteria • To information security change management process: evaluated risks of proposed changes • To information security risk assessment process itself: – Previous results from information security risk assessment – Previously identified information security status
Activities/functions	• Identify risk – Identify threats and their sources – Identify existing and planned controls – Identify relevant vulnerabilities – Identify risk owners • Identify consequences of risks – Identify consequences of incurred or realized risks

Process name	**Information security risk assessment process – derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2011)**
	– Assess business impact of risks • Assess likelihood of risks • Risk evaluation – compare levels of risk (consequences and likelihood) against evaluation and acceptance criteria
Metrics	• Numbers of identified and not identified (input from incident management process) risks • Numbers of acceptable and not acceptable risks • Time needed to assess planned changes • Resources used to assess risks
Owner	Information security officer
Manager	Information security officer or risk manager
Actors	Specialists, Consultants, Asset owners like line managers or process owners Legal advisors, Risk manager

Table 56 – Information security risk assessment process

12.3 Information security risk treatment process

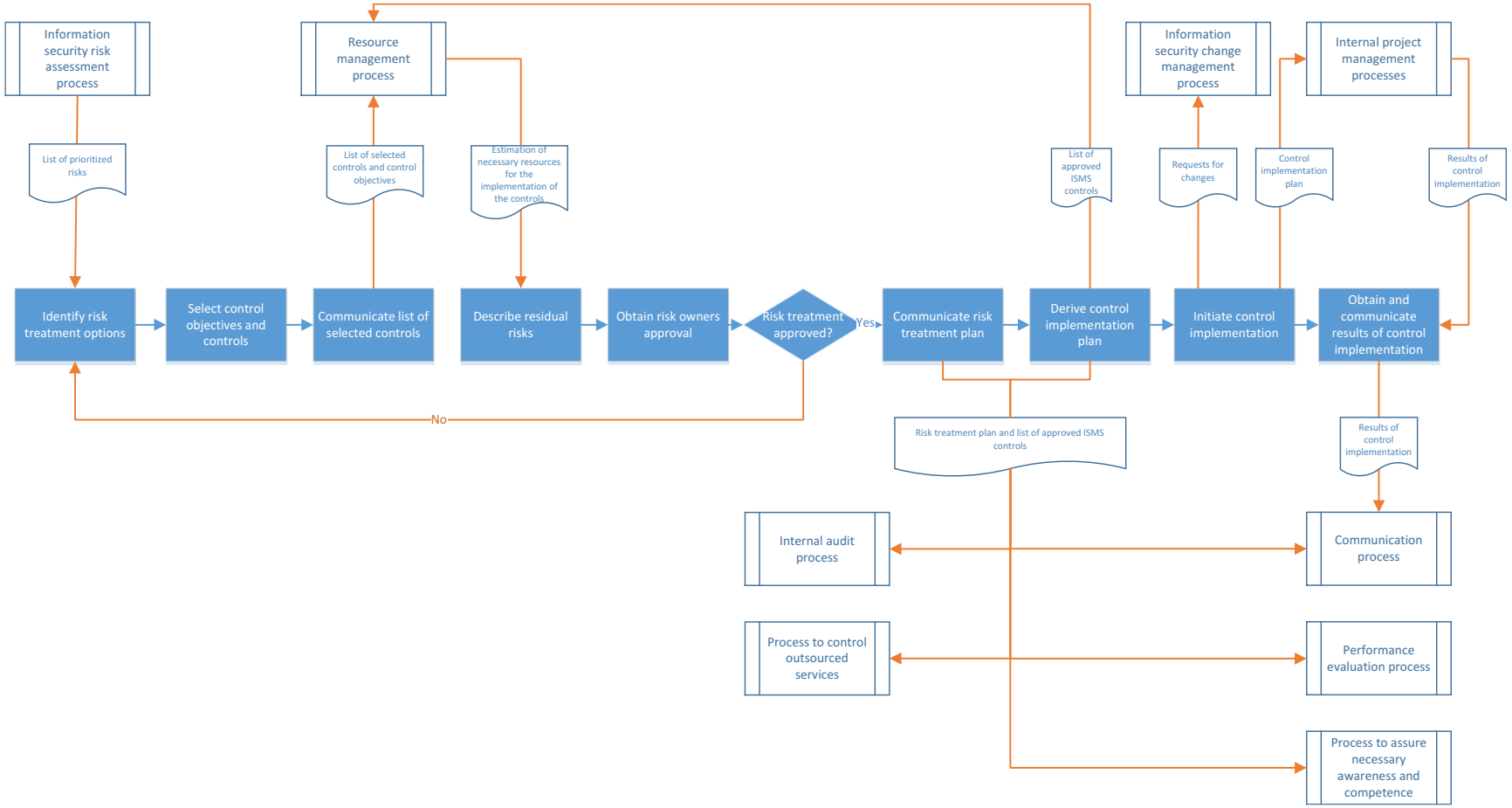

Figure 21 – Information security risk treatment process chart

Process Name	**Information security risk treatment process – derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2011)**
Process category	ISMS core process
Brief description	The information security risk treatment process is the process to identify and select risk treatment options including control objectives and controls.
Objectives/purposes	• identify and select appropriate risk treatment options • identify and select appropriate control objectives and controls
Input	• From information security risk assessment process: documented and evaluated risks in a list of prioritized risks • From resource management process: estimation of necessary resources for the implementation of the controls
Output	• To resource management process: selected controls and control objectives and list of approved ISMS controls • To process to control outsourced services, communication process, internal audit process, performance evaluation process, and process to assure necessary awareness and competence: risk treatment plan including acceptance of residual risks as well as a list with selected controls and control objectives • To information security change management process: requests for changes
Activities/functions	• Identify options for the treatment of risks • Select the control objectives and controls • Communicate list of selected controls to resource management process to obtain initial resource requirements – if necessary repeat this step and the selection of controls if necessary resources for a control are not appropriate. • Describe residual risks • Obtain risk owners approval for risk treatment plan • Derive control implementation plan from risk treatment plan including – Owner of the control/responsible person for the implementation – Priority – Tasks or activities to implement the control – Time target and resources for the implementation • Initiate control implementation • Obtain and communicate results of control implementation
Metrics	• Numbers of chosen risk treatment options • Numbers of not accepted residual risks • Time needed to produce the process outputs • Resources (time, money, etc.) needed to implement the

Process Name	Information security risk treatment process – derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2011)
	controls
Owner	Information security officer
Manager	Information security officer or risk manager
Actors	Specialists and Consultants Asset/risk owners like line managers or process owners Legal advisors and Risk manager

Table 57 – Information security risk treatment process

12.4 Resource management process

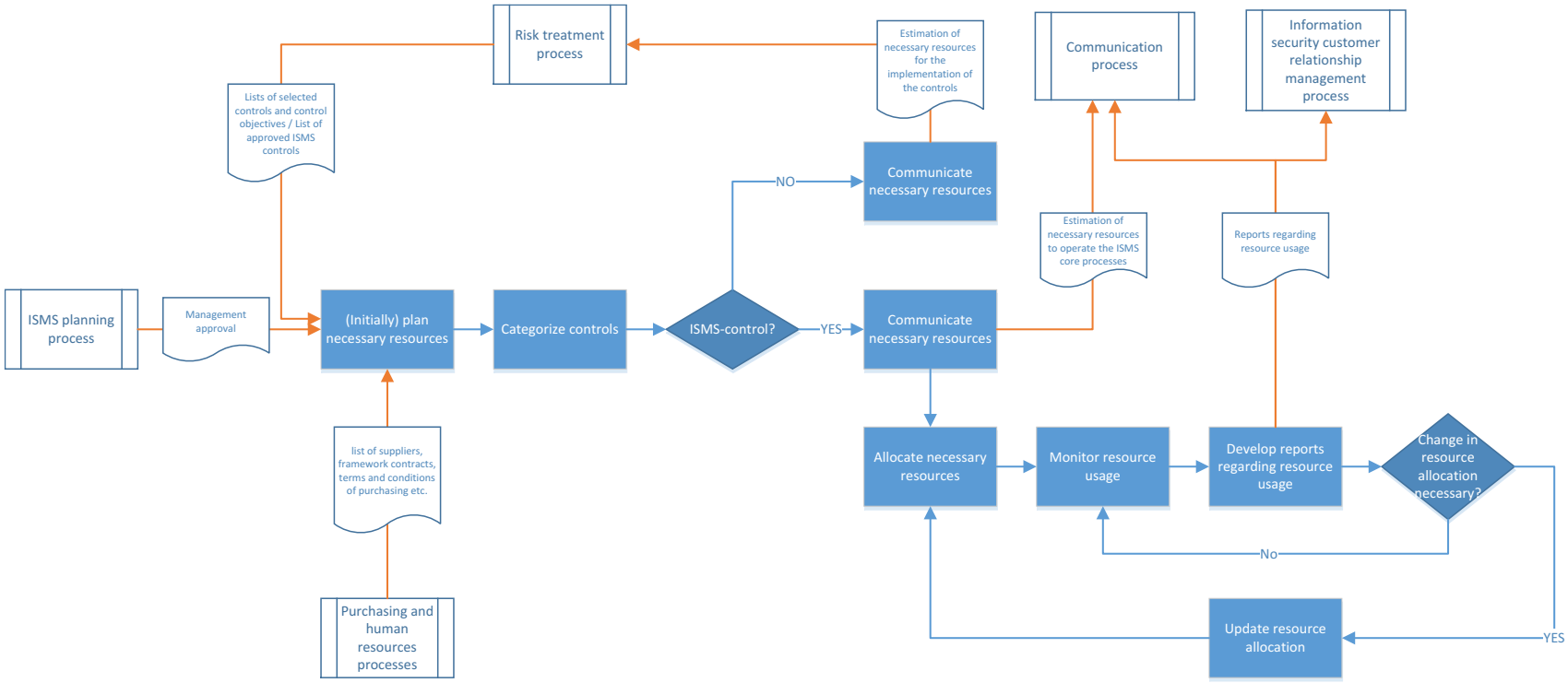

Figure 22 – Resource management process chart

Process Name	Resource management process
Process category	ISMS core process
Brief description	The resource management process is the process to identify, allocate and monitor required resources to run the ISMS core processes as well as to implement and run the selected controls.
Objectives/purposes	• Ensuring that the resources for the ISMS and the controls are available • Appropriate management of ISMS resources • Ensure efficiency of resource usage
Input	• From risk treatment process: Lists of selected controls and control objectives / List of approved ISMS controls • From ISMS planning process: Management approval for initiating the ISMS and documented business case for the ISMS / Project proposal • From purchasing department: list of suppliers, framework contracts, terms and conditions of purchasing etc.
Output	• For information security risk treatment process: Estimation of necessary resources to implement controls • For communication process: Estimation of necessary resources to operate the ISMS core processes and reports regarding resource usage of ISMS core processes • For information security customer relationship management process: reports on resource usage
Activities/functions	• (Initially) plan necessary resources to implement and run the controls • Categorize controls – a differentiation is made between controls funded by the ISMS budget and controls funded by other departments • Communicate necessary resources – to the information security risk treatment process to implement and run the controls – if necessary repeat this step and the planning of necessary resources if necessary – to the communication process – regarding the ISMS controls (necessary to operate the ISMS core processes) • Allocate necessary resources for approved controls which are funded by the ISMS • Permanently monitor ISMS resource usage and if necessary update resource allocation • Develop and communicate reports regarding resource usage of ISMS core processes to the information security officer
Sample Metrics	• Resources (time, money, human resources) needed to implement the selected controls • Planned but not used resources and resource trends • Number of controls with budget overrun • Ratio between ISMS funded controls and controls funded by other departments
Owner	Information security officer

Process Name	Resource management process
Manager	Information security officer or resource manager
Actors	Information security officer or resource manager Purchase and human resources department, Consultants and Specialists

Table 58 – Resource management process

12.5 Process to assure necessary awareness and competence

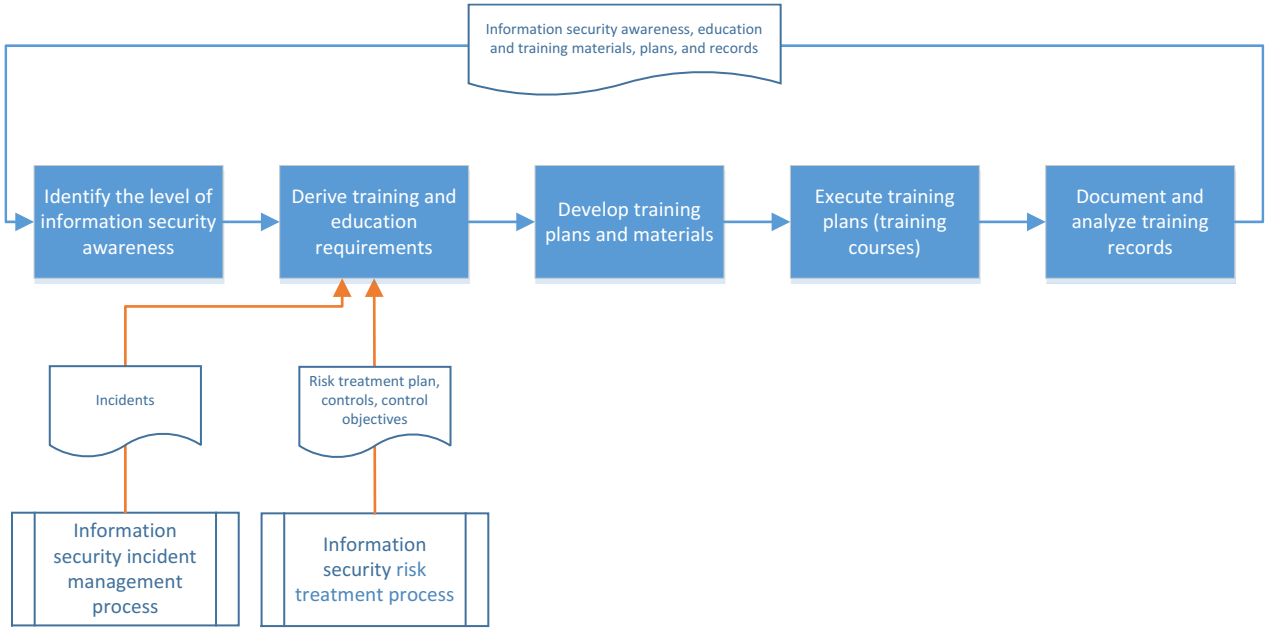

Figure 23 – Process to assure necessary awareness and competence process chart

Process Name	Process to assure necessary awareness and competence – derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013)
Process category	ISMS core process
Brief description	Development and implementation of an information security awareness, training and education program.
Objectives/purposes	To ensure that all personnel receives the necessary security training and/or education. Employees shall be aware of the information security policy, their contribution to the effectiveness of ISMS including the benefits of improved information security performance and implications of not conforming with ISMS requirements.
Input	• From ISMS planning process: – ISMS objectives, priorities and organizational requirements – ISMS scope, boundaries and policy Organization structure, roles, responsibilities, standards and procedures for information security • From the information security incident management process: incidents • From information security risk treatment process: – Risk treatment plan, controls, control objectives • From the process to assure necessary awareness and competence itself: – Information security awareness, education and training materials, plans, and records (also from preliminary results of the Process to assure necessary awareness and competence)
Output	• For the process to assure necessary awareness and competence itself – Information security awareness education and training plans, – Information security awareness education and training materials – Information security awareness education and training records
Activities/functions	• Identify the level of information security awareness • Derive training and education requirements for each unit/department • Develop training plans and materials – also integrate information security awareness in other training courses • Execute training plans (training courses) • Document and analyze training records
Metrics	• Annual resources (time, money, human resources) needed to implement the training program • Resources spent for information security training and awareness per operational and administrative unit

Process Name	Process to assure necessary awareness and competence – derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013)
	• Necessary resources to develop and maintain training materials • Ratio between already trained and not trained employees • Number of employees who failed tests at the end of training courses
Owner	Information security officer
Manager	Information security awareness officer
Actors	Information security officer Information security awareness officer Information security awareness training team including trainers External trainers

Table 59 – Process to assure necessary awareness and competence

12.6 Communication process

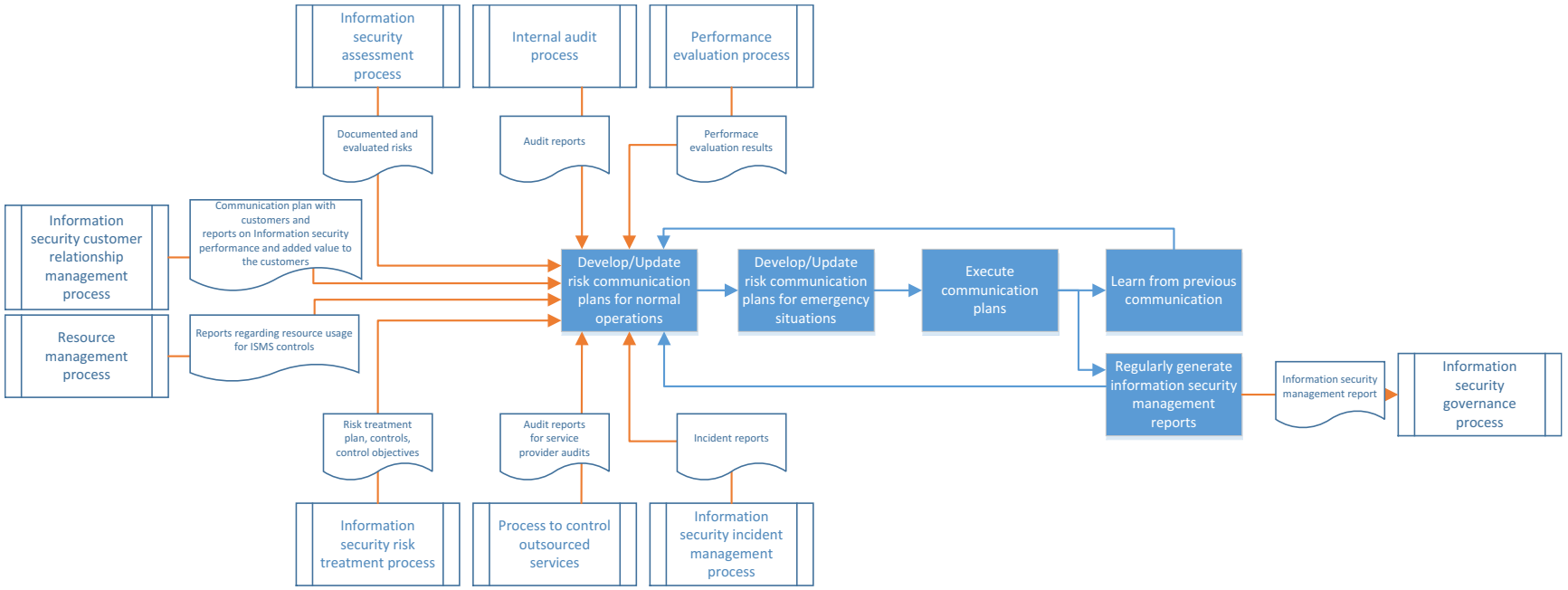

Figure 24 – Communication process chart

Process Name	**Communication process – derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2011)**
Process category	ISMS core process
Brief description	Risk communication is the process to achieve agreement on how to manage risks by exchanging and/or sharing all information about risks between the decision-maker and other stakeholders.
Objectives/purposes	• Continual understanding of the organizations information security risk management process and results • Provide assurance of the outcome of the organizations risk management • Collect risk information, support decision making, improve awareness • Share results from risk assessment and risk treatment process • Avoid or reduce both occurrence and consequence of information security breaches due to the lack of mutual understanding among decision makers and stakeholders • Obtain new information security knowledge • Co-ordinate with other parties and plan responses to reduce consequences of any incident • Give decision makers/stakeholders a sense of responsibility about risks
Input	• From ISMS planning process: – Established committee to debate about risks • From information security risk assessment process: – Documented risks (threats and vulnerabilities) – Documented evaluation of risks (consequences, business impact, likelihood and comparison against risk criteria) in a list of prioritized risks as well as documented risk owners • From information security risk treatment process: – Risk treatment and control implementation plan – List with selected controls and control objectives – Acceptance of residual risks • From documentation and records control process: – Appropriate documents and necessary records • Input for information security management reports: – From resource management process: Reports regarding resource usage for ISMS controls – From requirements management process: changes in requirements – From internal audits and performance evaluation process: audit and performance reports – From process to control outsourced services: audit reports

Process Name	Communication process – derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2011)
	– From incident management process: incident reports • From information security customer relationship management process: communication plan with customers and reports on information security performance and added value to the customers
Output	• To information security governance process: information security management reports
Activities/functions	• Develop/Update risk communication plans for normal operations (what need to be communicated to whom, when and who will communicate? – for example incidents, regulations, requirements, tasks, responsibilities; cooperate with public relations or communications department) • Develop/Update risk communication plans for emergency situations • Execute communication plans (Relevant information as defined in the communication plans to recipients as defined in the communication plan) • Learn from previous communication • Regularly generate information security management reports
Metrics	• Annual resources (time, money, human resources) needed to communicate risks • Resources spent to develop and maintain communication plans
Owner	Information security officer
Manager	Information security officer
Actors	Information security officer Stakeholders/Risk owners Public relations or communications department

Table 60 – Communication process

12.7 Documentation and records control process

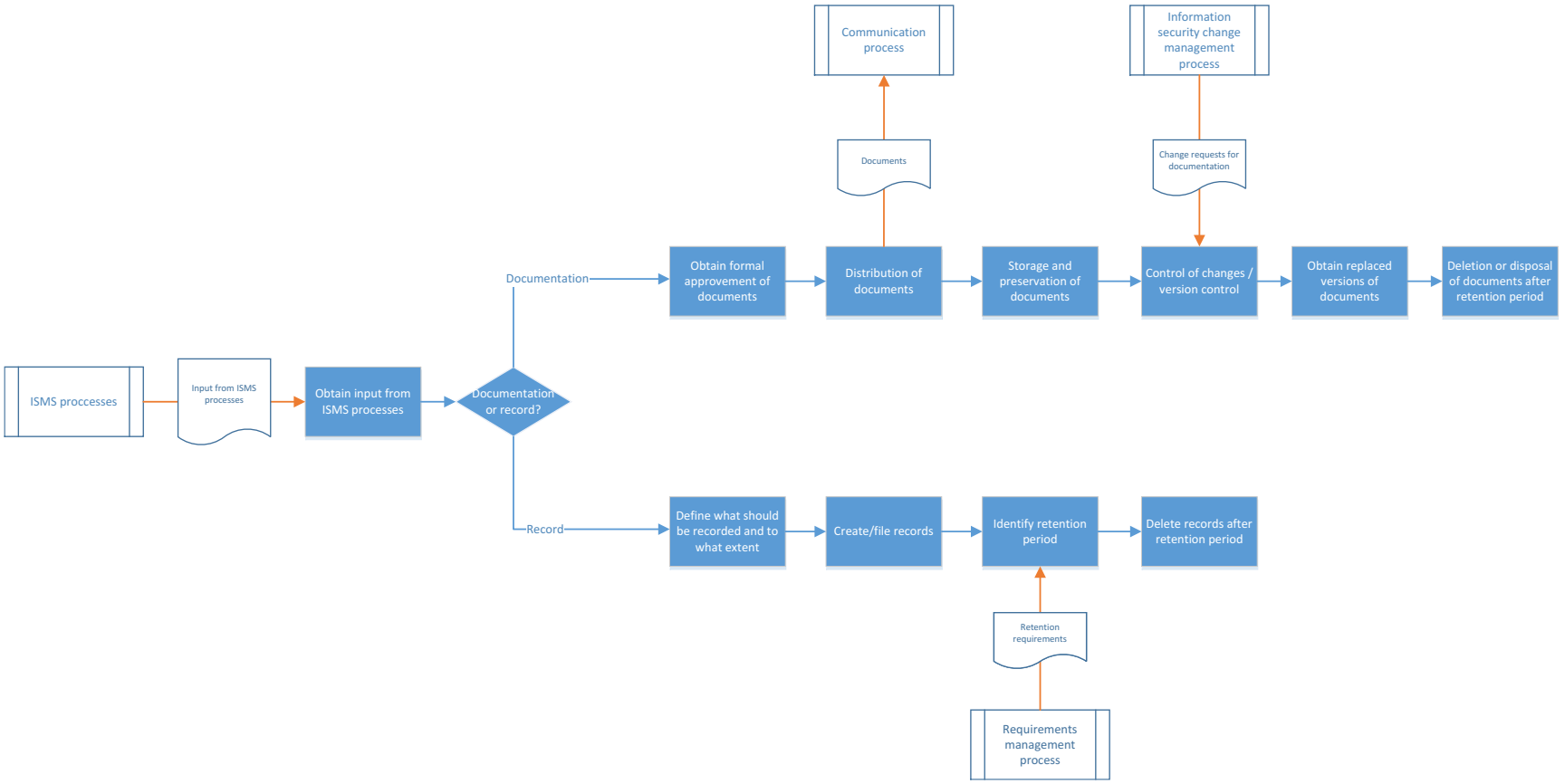

Figure 25 – Documentation and records control process chart

Process Name	**Documentation and records control process – derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013)**
Process category	ISMS core process
Brief description	Documentation and records control process is the process to identify, create, update and control information determined to be necessary for the effectiveness of the ISMS.
Objectives/purposes	• Ensure that all information determined to be necessary for the effectiveness of the ISMS are documented • Ensure appropriate identification, description, format, review and approval for suitability and adequacy of documents and records • Ensure that the relevant documented information is available for use, where and when it is needed and it is adequately protected • Records are protected from loss, destruction, falsification, unauthorized access and unauthorized release
Input	• From ISMS planning process: – ISMS documentation framework including a summary of requirements for ISMS documentation and records control – Established administrative procedure of ISMS document management – Repositories and templates for required records and documents of the ISMS • All output from other information security risk assessment and treatment process (as basis for documentation – for example from information security risk treatment process: records and documentation of the results of implementation) • From change management process: necessary changes of documents • From requirements management process: retention requirements
Output	• For all ISMS processes: Appropriate documents and necessary records
Activities/functions	• Obtain input from ISMS processes • Documentation: – Obtain formal approval of documents – Distribution of documents (via communication process) – Storage and preservation, including preservation of legibility – Control of changes/version control – Obtain replaced versions of documents – Deletion or disposal of documents after retention period • Records:

Process Name	Documentation and records control process – derived mainly from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013)
	– Define what should be recorded, to what extent – Create/file records – Identify period of retention (partially available as input from the requirements process) – Delete records after retention period
Metrics	• Number of changed and re-communicated documents per period • Number of disposed documents and records • Number(s) of records • Number of documents which initially not fulfill the requirements of the ISMS documentation framework • Number of templates
Owner	Information security officer
Manager	Information security officer
Actors	Information security officer Change management Control implementers Public relations or communications department

Table 61 – Documentation and records control process

12.8 Requirements management process

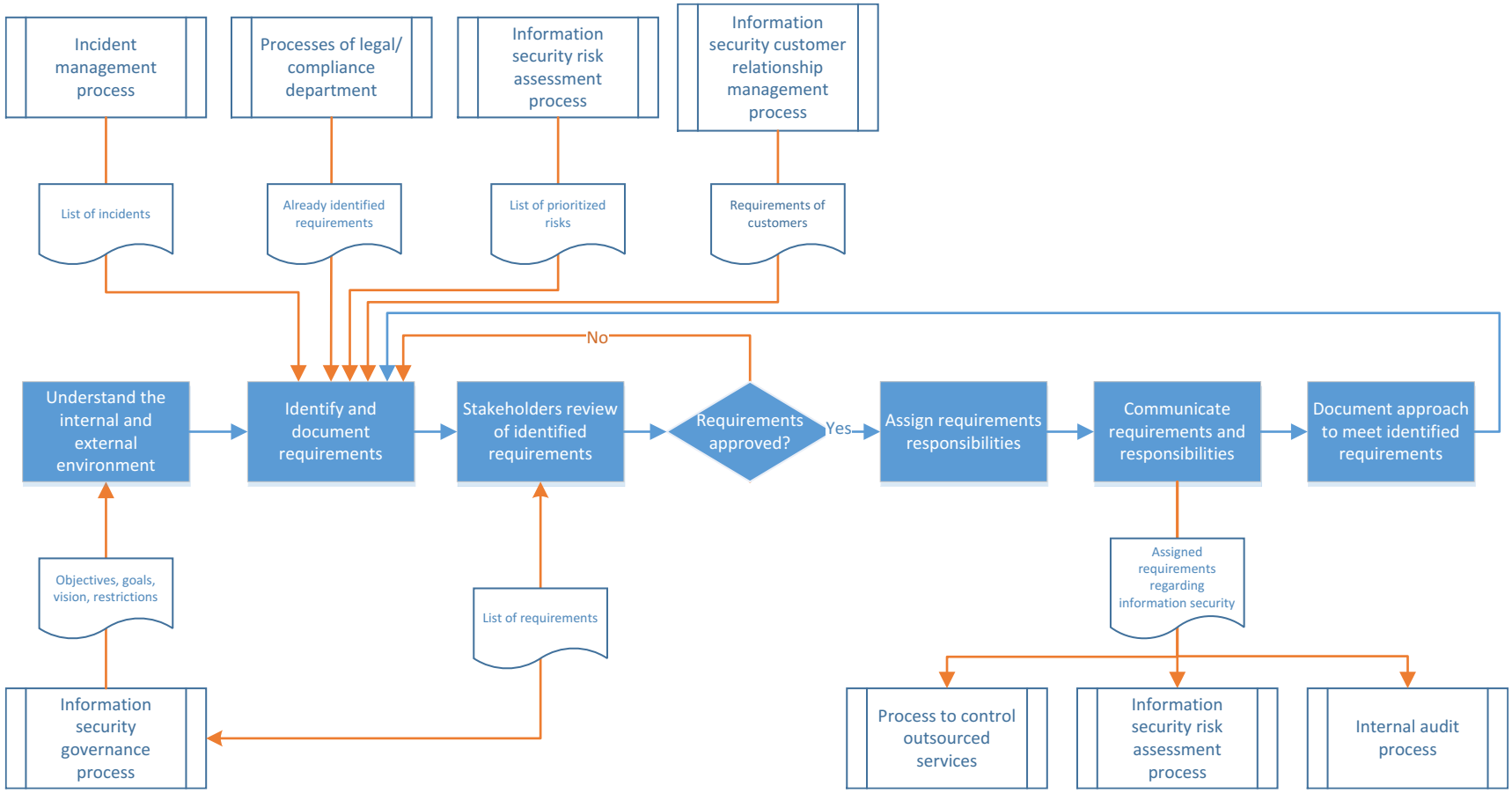

Figure 26 – Requirements management process chart

Process Name	**Requirements management process – mainly derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (Information Systems Audit and Control Association, n.d.-c)**
Process category	ISMS core process
Brief description	Requirements management process is the process to ensure an up-to-date understanding of the needs and expectations of interested parties relevant to information security and the ISMS.
Objectives/purposes	• All relevant legislative statutory, regulatory, contractual requirements are met • The information security related requirements are included in the requirements for – Business processes and internal regulations – new information systems – enhancements to existing information systems – contracts with suppliers and service providers
Input	• From information security risk assessment process: – While providing information about legal, statutory, regulatory and contractual requirements to the information security risk assessment process, the information security risk assessment process also provides input for the identification of requirements. • From information security governance process (stakeholders): – Objectives, goals, vision, restrictions • From legal/compliance department processes: already identified requirements • From information security customer relationship management process: requirements of customers • From incident management process: list of incidents
Output	• To internal audit process, the information security risk assessment process, and the process to control outsourced services: Documented and assigned requirements regarding information security including a list of the legislative and regulatory references including contracts and agreements applicable to the organization (International Organization for **Standardization and International Electrotechnical Commission**, 2011, p. 34)
Activities/functions	• Understand the internal and external environment of the organization and the ISMS (Information Systems Audit and Control Association, n.d.-c, p. 87) • Identify and document requirements – Identification of applicable legislation and contractual requirements – Identification of requirements from assessed risks

Process Name	Requirements management process – mainly derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (Information Systems Audit and Control Association, n.d.-c)
	(current and projected information security threat environment). – Identification of requirements from principles, objectives, and business requirements for information handling, processing, storing, communicating and archiving. – Identification of requirements from incidents – Identification and prioritization of conflicting requirements • Stakeholders review and approval of identified requirements • Assign responsibilities to meet the requirements • Communicate requirements and responsibilities • Document approach to meet identified requirements • Keep requirements up to date (start process again)
Metrics	• Number of relevant requirements • Resources spent to identify, document and maintain requirements
Owner	Information security officer
Manager	Information security officer
Actors	Business managers Information security officer Staff of legal department Risk managers Stakeholders

Table 62 – Requirements management process

12.9 Information security change management process

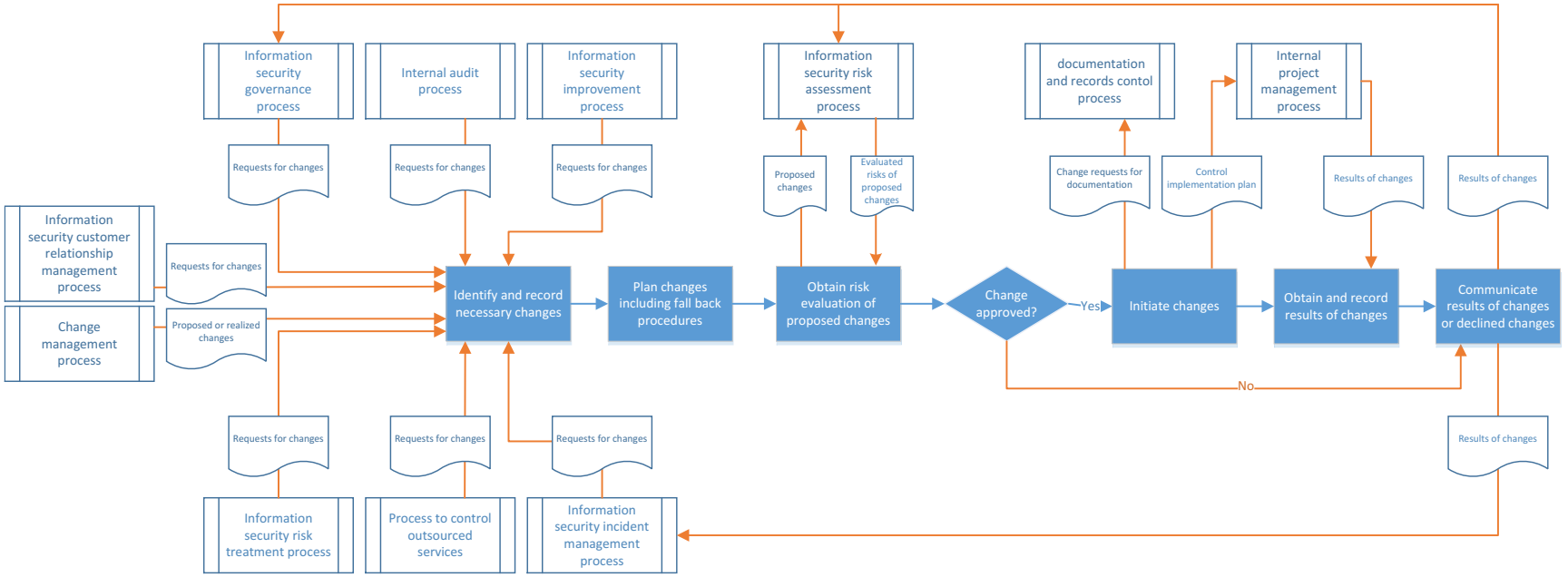

Figure 27 – Information security change management process chart

Process Name	**Information security change management process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2013) (International Organization for Standardization and International Electrotechnical Commission, 2013)**
Process category	ISMS core process
Brief description	Information security change management process is the process to control changes of ISMS elements and review the consequences of unintended changes. This process only focusses on change management of the ISMS. This process is linked with a general change management process of the organization which provides input (proposed or realized changes) to this process.
Objectives/purposes	To mitigate any adverse effects of changes as necessary. Relevant changes like changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled from the perspective of information security.
Input	• From information security governance process: requests for changes as part of the management reviews (Results of changes, internal audits, status of outsourced processes as well as monitoring and evaluation results are reviewed within the information security governance process) • From information security incident management process: requests for changes to deal with incidents • From information security risk assessment process: evaluated risks of proposed changes • From information security customer relationship management process: requests for changes • From information security risk treatment process: requests for changes • From internal audit process: requests for changes (to correct nonconformities) • From process to control outsourced services: request for changes (to correct nonconformities) • From information security improvement process: requests for changes as results of the continual improvement • From change management process: proposed or realized changes – in external or internal issues relevant to the ISMS, – of employment responsibilities, – of organization, business processes, information processing facilities and systems, operating platforms, software, – of operational environment, – of supplier services,

Process Name	Information security change management process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2013) (International Organization for Standardization and International Electrotechnical Commission, 2013)
	– goals, objectives and stakeholders expectations
Output	• To information security governance process: Results of changes, internal audits, status of outsourced processes as well as monitoring and evaluation results are reviewed within the information security governance process. • To information security incident management process: status/results of changes • To information security risk assessment process: initiation of risk assessment when significant changes are proposed or occur; results of changes • To documentation and records control process: Necessary changes (control implementation plan) • To internal project management process: Necessary changes (control implementation plan)
Activities/functions	• Identify and record necessary changes of – Controls – ISMS processes – ISMS documentation – ISMS scope, policy, standards procedures • Plan changes including fall back procedures • Obtain risk evaluation of proposed changes from risk assessment process (assessment of potential impacts) • Approve or decline changes • Initiate changes via documentation and records control process or internal project management processes • Obtain and record results of changes • Communicate results of changes to risk assessment process
Metrics	• Numbers and ratio of approved/declined changes • Time needed to produce the process outputs
Owner	Information security officer
Manager	Information security change responsible or Information security officer
Actors	Information security officer Information security change responsible

Table 63 – Information security change management process

12.10 Process to control outsourced services

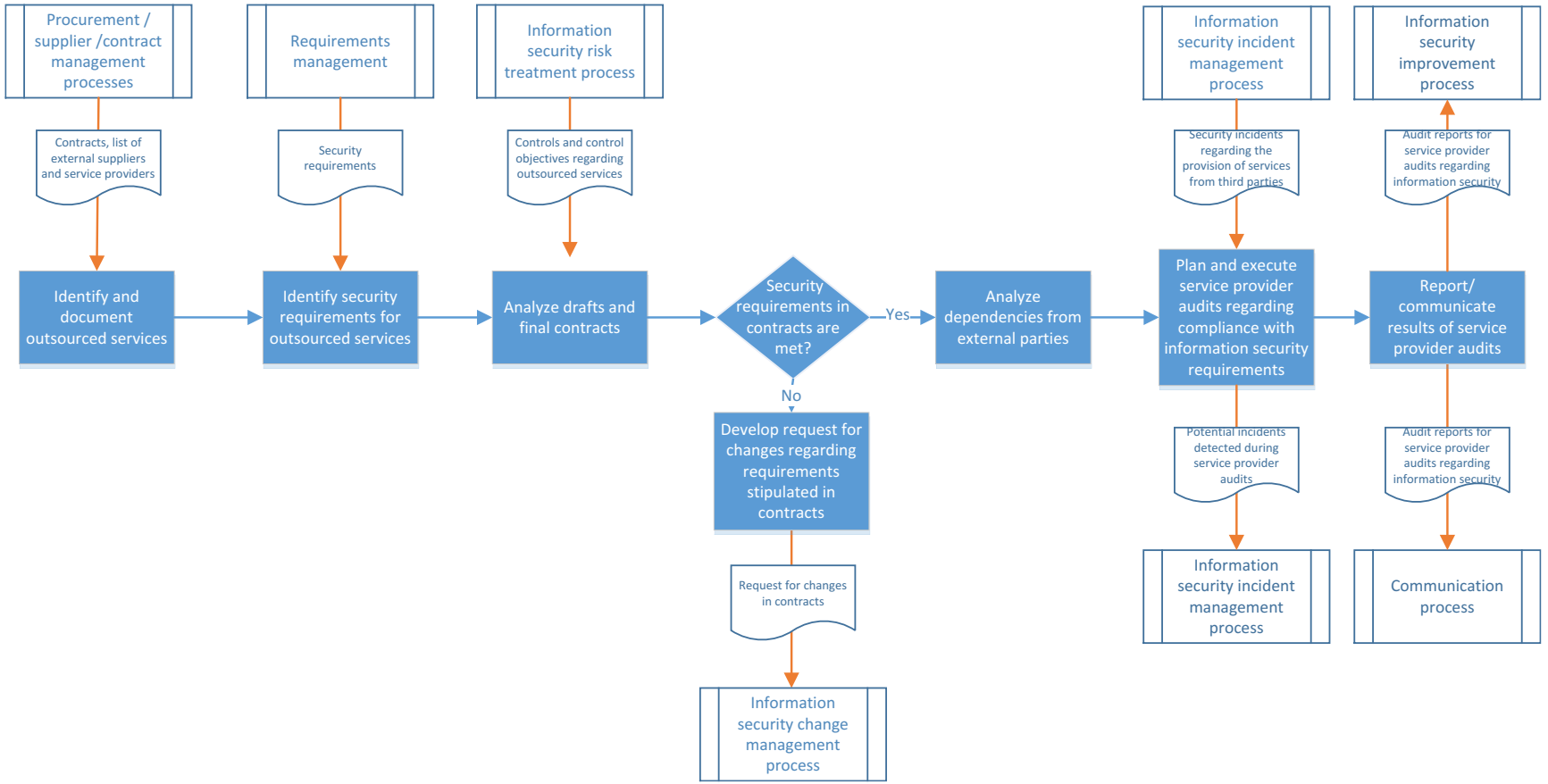

Figure 28 – Process to control outsourced services process chart

Process Name	**Process to control outsourced services – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2013)**
Process category	ISMS core process
Brief description	The process to control outsourced services is the process to ensure that outsourced services are determined and controlled. This includes identification and documentation of outsourced services as well as dependencies from external parties.
Objectives/purposes	To mitigate any adverse effects of outsourced services and to ensure that information provided to external service providers are processed in compliance with the information security requirements of the outsourcing organization.
Input	• From requirements management process: applicable security requirements • From procurement/supplier/contract management processes: contracts, list of external suppliers and service providers; overview of outsourced services including contractual agreements and assessed dependencies • From security risk treatment process: controls and control objectives regarding outsourced services • From information security incident management process: (potential) security incidents regarding the provision of services from third parties
Output	• For information security change management process: Request for changes - Initiation of necessary changes in contracts or of service providers • For documentation and records control process: Audit program and plans for service provider audits regarding information security, audit results (not displayed in process chart) • For communication process (management review and improvement process): Audit reports for service provider audits regarding information security • For information security incident management process: direct information of potential incidents detected during service provider audits • For information security improvement process: audit reports of service provider audits
Activities/functions	• Identify and document outsourced services • Identify security requirements for outsourced service • Analyze drafts or final contracts if security requirements are met (Ensure that information security requirements are addressed properly in the contracts) • Develop request for changes regarding requirements stipulated in contracts

Process Name	Process to control outsourced services – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2013)
	• Analyze dependencies from external parties • Plan and execute service provider audits regarding compliance with information security requirements • Report/communicate results of service provider audits
Metrics	• Numbers of service providers • Numbers of initiated and implemented changes in contracts or of service providers • Number of service provider audits and findings • Annual resources (time, money, human resources) needed to manage information security in outsourced services
Owner	Information security officer
Manager	Information security officer
Actors	Information security officer Internal auditors for service provider audits Staff of legal department

Table 64 – Process to control outsourced services

12.11 Performance evaluation process

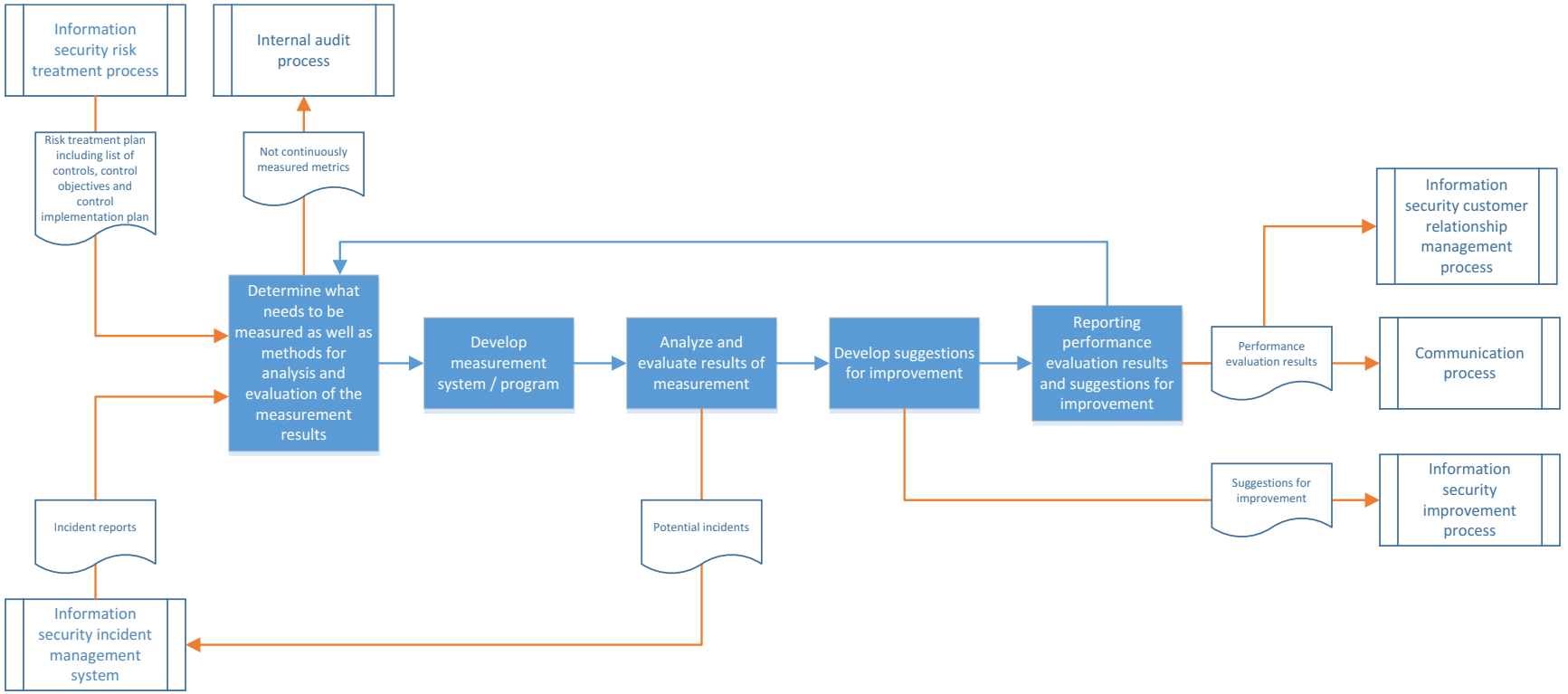

Figure 29 – Performance evaluation process chart

Process Name	**Performance evaluation process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2010b)**
Process category	ISMS core process
Brief description	The performance evaluation process contains monitoring, measurement, analysis and evaluation of two main criteria. First, the performance of the security controls and second the performance of the ISMS processes. Performance measurement differs from performance audit (internal audit) which is performed independently.
Objectives/purposes	The performance of ISMS need to be monitored in terms of verification and reporting of security control implementation as well as the information security management processes. Objective of this process is to assess the performance against the policy and objectives of the organization (International Organization for Standardization and International Electrotechnical Commission, 2014, p. 11) to support management review (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 62)
Input	• From ISMS planning process: ISMS policy (not displayed in process chart) • From information security risk treatment process: Risk treatment plan including list of controls, control objectives and control implementation plan. This process should especially integrated/linked with the information security risk treatment process because metrics for controls should be defined as soon as possible within the planning of controls to avoid unnecessary costs afterwards. • From incident management process: incident reports are used to verify/evaluate control functionality
Output	• For communication process and information security customer relationship management process.: reporting performance evaluation results • For information security incident management process: potential incidents • For Information security improvement process: suggestions for improvement • For documentation and records control process: measurement results (not displayed in process chart) • For the internal audit process: Where metrics are not continuously measured this process could also be linked with the internal audit process as it provides requirements

Process Name	Performance evaluation process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2010b)
	to measure metrics within internal audits.
Activities/functions	• Determine and regularly review what needs to be measured as well as methods for analysis and evaluation of the measurement results • Develop measurement system / program (what needs to be measured, methods for measurement, when should the measurement be performed, who shall measure) (International Organization for Standardization and International Electrotechnical Commission, 2010b, p. 13) • Analyze and evaluate results of measurement • Develop suggestions for improvement • Reporting performance evaluation results and suggestions for improvement
Metrics	• Measured metrics per process/control • Overall count of metrics measured • Resources needed to perform measurement • Resources needed to perform analysis and evaluation • Annual resources (time, money, human resources) needed to perform the process (differentiated between ISMS performance evaluation and security control performance evaluation.
Owner	Information security officer
Manager	Information security officer (for the performance measurement of ISMS processes) and process managers, line managers or process owners for the performance evaluation of security controls within their responsibility.
Actors	Information security officer Users Persons in charge of information systems Process managers Line managers Process owners

Table 65 – Performance evaluation process

12.12 Internal audit process

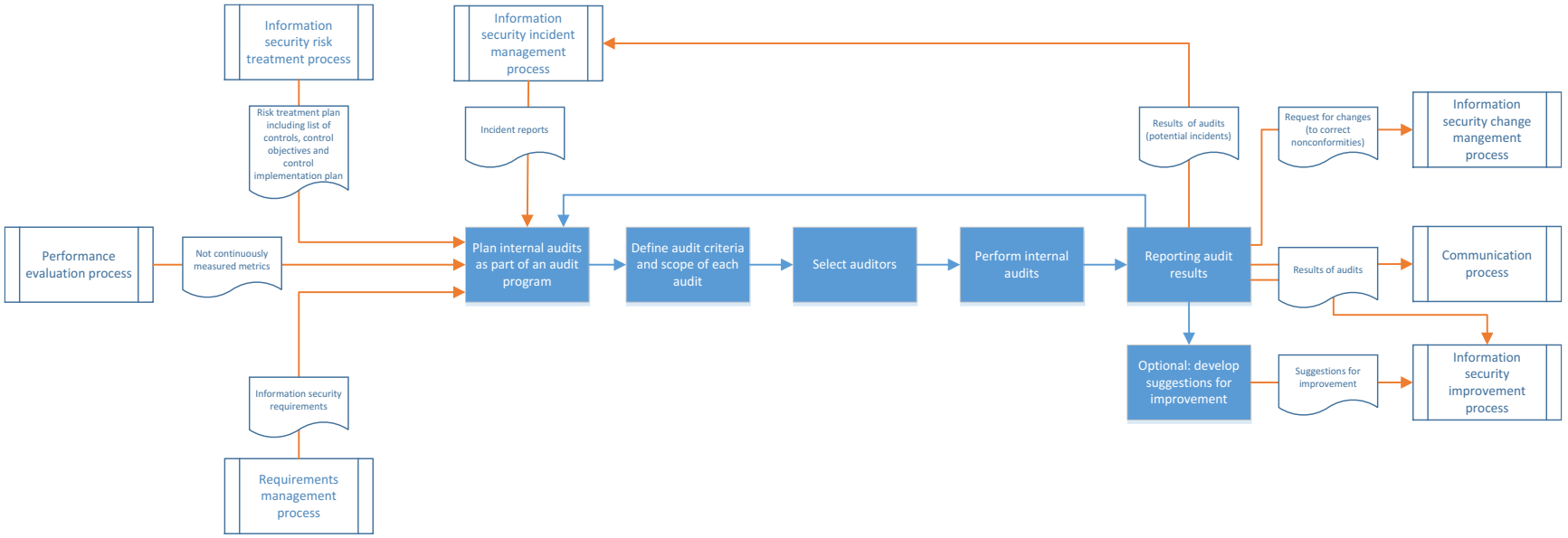

Figure 30 – Internal audit process chart

Process Name	**Internal audit process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2013)**
Process categorization	ISMS core process
Brief description	Effectiveness and efficiency of the ISMS and implemented controls are examined independently within the scope of internal audits (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 55) The ISMS core process of internal auditing contains only the part of auditing information security controls. The audit of the ISMS processes should be performed independent from the ISMS operation.
Objectives/purposes	ISMS audit should be performed to validate the ISMS against the needs of the business and to maintain the commitment of the business to the ISMS (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 41). The internal audit process is to determine effectiveness and performance of control objectives, controls (…and ISMS processes – but this is not a part of this process – see 5.1) as well as to identify non-conformities to the requirements – especially standards, legislation or regulations and identified security requirements (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 55).
Input	• From documentation and records control process: results of former audits (not displayed in the process chart) • From ISMS planning process: ISMS policy (not displayed in the process chart) • From requirements management process: information security requirements • From information security risk treatment process: risk treatment plan including list of controls, control objectives and control implementation plan • From incident management process: incident reports are used to verify/evaluate control functionality • From performance evaluation process: not continuously measured metrics
Output	• For communication process: reporting internal audit results • For information security improvement process: results of audits and suggestions for improvement • For information security change management process:

Process Name	Internal audit process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (International Organization for Standardization and International Electrotechnical Commission, 2013)
	request for changes regarding nonconformities of information security controls • For documentation and records control process: internal audit results (not displayed in the process chart) • For information security incident management process: potential incidents
Activities/functions	• Plan internal audits as part of an audit program • Define audit criteria and scope of each audit • Select auditors • Perform internal audits • Optional: develop suggestions for improvement (to improve efficiency, effectiveness of controls or to eliminate causes of nonconformities) • Reporting internal audit results to communication process and information security improvement process, to information security incident management process (as results are possibly potential incidents) and to information security change management process (to initiate necessary changes to correct nonconformities)
Metrics	• Resources needed to perform internal audits • Count of identified non-conformities or improvement options (for ISMS, for controls, per audit, per year) • Annual resources (time, money, human resources) needed to perform the process (differentiated between ISMS process audit and security controls audit.
Owner	Information security officer (audit of security controls) and top management (audit of ISMS processes)
Manager	Information security officer (audit of security controls) and internal audit department (audit of ISMS processes)
Actors	Information security officer External or internal auditors Process owners and managers Line managers Process owners

Table 66 – Internal audit process

12.13 Information security governance process

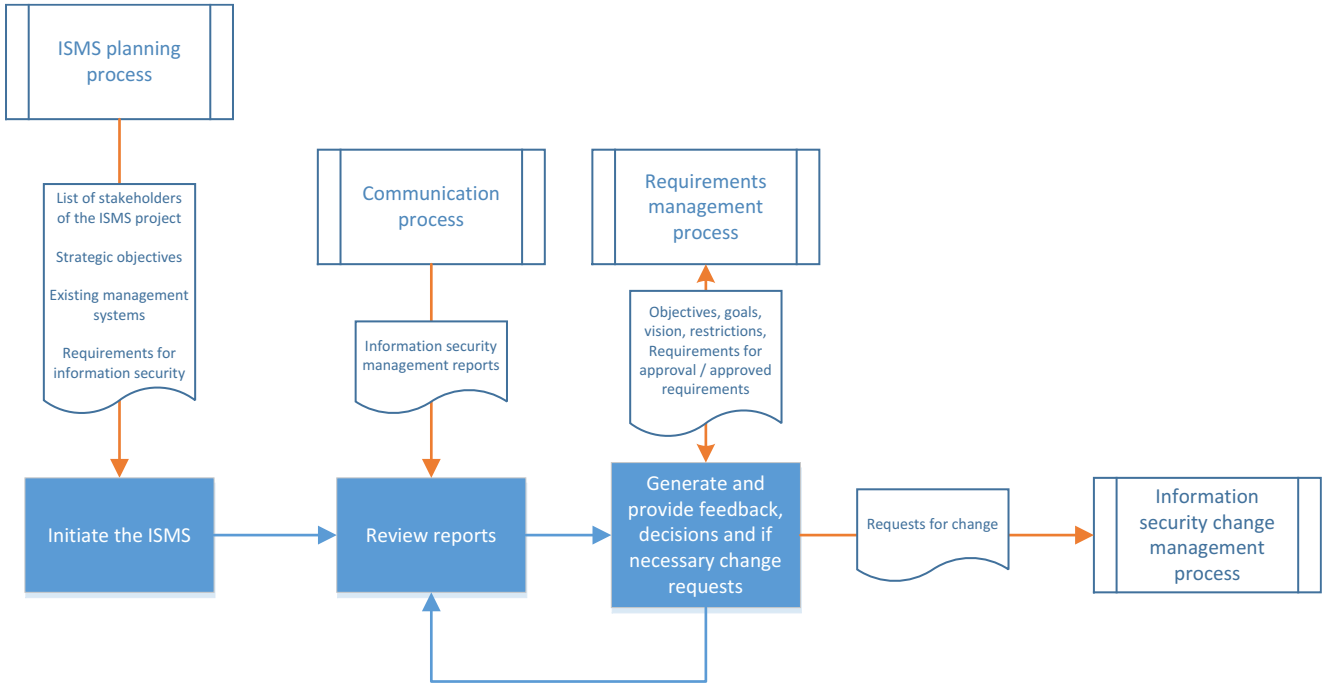

Figure 31 – Information security governance process chart

Process Name	**Information security governance process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (Information Systems Audit and Control Association, n.d.-c)**
Process category	Management process
Brief description	The management should initiate management reviews of the ISMS including information security controls where necessary to ensure that the ISMS as well as the information security level meets the objectives (involvement and commitment (International Organization for Standardization and International Electrotechnical Commission, 2010a, p. 40)) of the top management.
Objectives/purposes	Objective of this process is to ensure an alignment of the ISMS with the objectives and needs of the governing stakeholders.
Input	• From requirements management process: changed requirements • From communication process: information security management reports containing – Former management reports – Status of actions from former management reports – Changes in requirements – Audit reports – Incident reports • From ISMS planning process: – List of stakeholders of the ISMS project, – strategic objectives, – existing management systems, – requirements for information security
Output	• For documentation and records control process: decisions related to the governance of the ISMS (not displayed in the process chart • For information security change management: change requests •
Activities/functions	• Initiate the ISMS • Review reports (measurement, audit reports, results of risk assessment and status of risk treatment plan and feedback from interested parties) • Generate management feedback, decisions and if necessary change requests
Metrics	• Decision memos accepted and rejected by the management • Count of changes initiated by the top management
Owner	Top management
Manager	Information security officer

Process Name	**Information security governance process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (Information Systems Audit and Control Association, n.d.-c)**
Actors	Top management Information security officer

Table 67 – Information security governance process

12.14 Information security incident management process

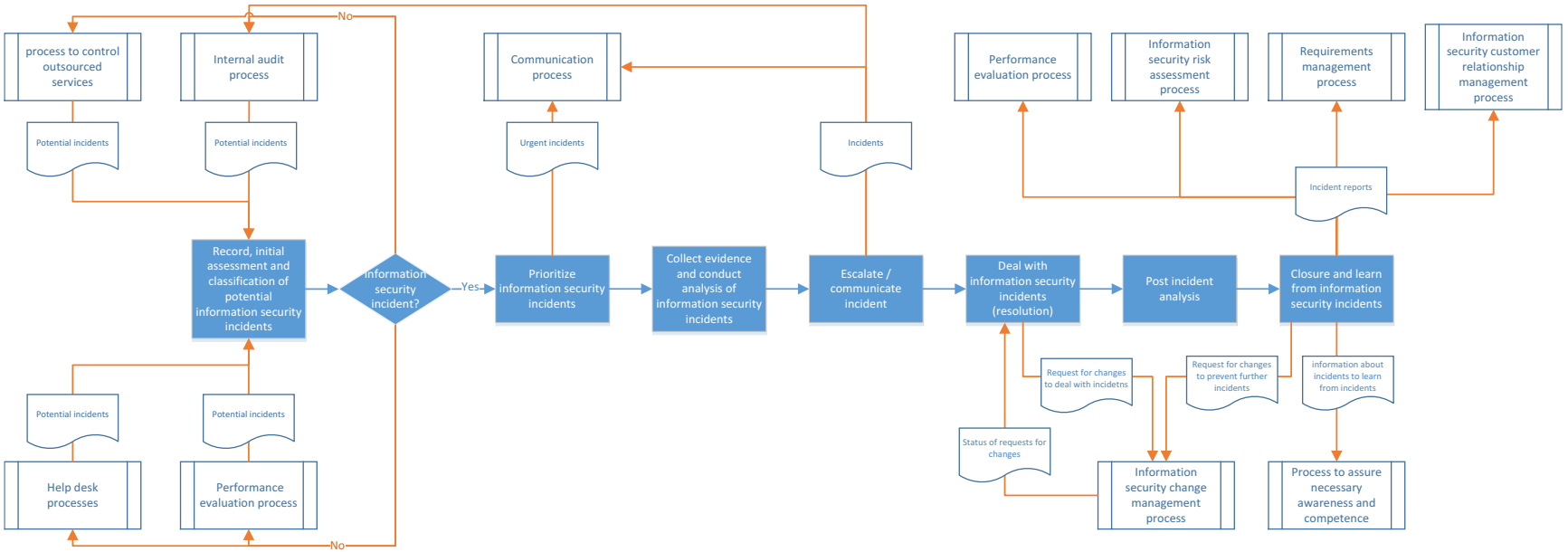

Figure 32 – Information security incident management process chart

Process Name	**Information security incident management process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2011)**
Process category	ISMS core process
Brief description	According to (International Organization for Standardization and International Electrotechnical Commission, 2014, p. 3) an information security incident is a single or series of unwanted or unexpected information security events (possible breach of information security, policy or failure of controls) that have a significant probability of compromising business operations and threatening information security. The information security incident management process is for detecting, reporting, assessing, responding to, dealing with and learning from information security incidents.
Objectives/purposes	The objective of this process is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 20). Further objectives are to ensure a quick, effective and orderly response to information security incidents (International Organization for Standardization and International Electrotechnical Commission, 2013, p. 20).
Input	• Employees and contractors should report potential weaknesses and incidents as they detect them: – From help desk processes (employees): potential incidents – From process to control outsourced services (contractors): potential incidents • From internal audit process: potential incidents • From performance evaluation process: potential incidents • From documentation and records control process: information needed to assess the incident (not displayed in the process chart) • From process to control outsourced services: potential incidents • Form information security change management process: status of requests for changes
Output	• To communication process: incidents • To information security change management process: Request for changes to respond to/deal with and to prevent further incidents • To process to assure necessary awareness and competence:

Process Name	Information security incident management process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2011)
	information about incidents to learn from incidents • To information security risk assessment process: information about risks to be considered in the evaluation of risks. • To documentation and records control process: information regarding the incident (evidence, results of incident assessment, et cetera – not displayed in the process chart) • To internal audit process: incidents • To performance evaluation process: incidents • To information security customer relationship management process: incidents
Activities/functions	• Recording, initial assessment and classification (decision to classify as Information security incident or not) of potential information security incidents • Prioritize information security incidents • Report information security incidents (as quickly as possible) • Respond to information security incidents: – collect evidence and conduct analysis of information security incidents – escalate (if required) and communicate incident – deal with information security incidents (resolution) – post incident analysis • Closure and learn from information security incidents (reduce likelihood or impact of future incidents)
Metrics	• Incidents per time period • Mean time to manage an incident • Annual resources (time, money, human resources) needed to manage incidents • Losses caused by incidents • Count of change requests caused by incident handling
Owner	Information security officer
Manager	Information security officer or incident manager
Actors	Information security officer Experts assessing and responding to incidents

Table 68 – Information security incident management process

12.15 Information security improvement process

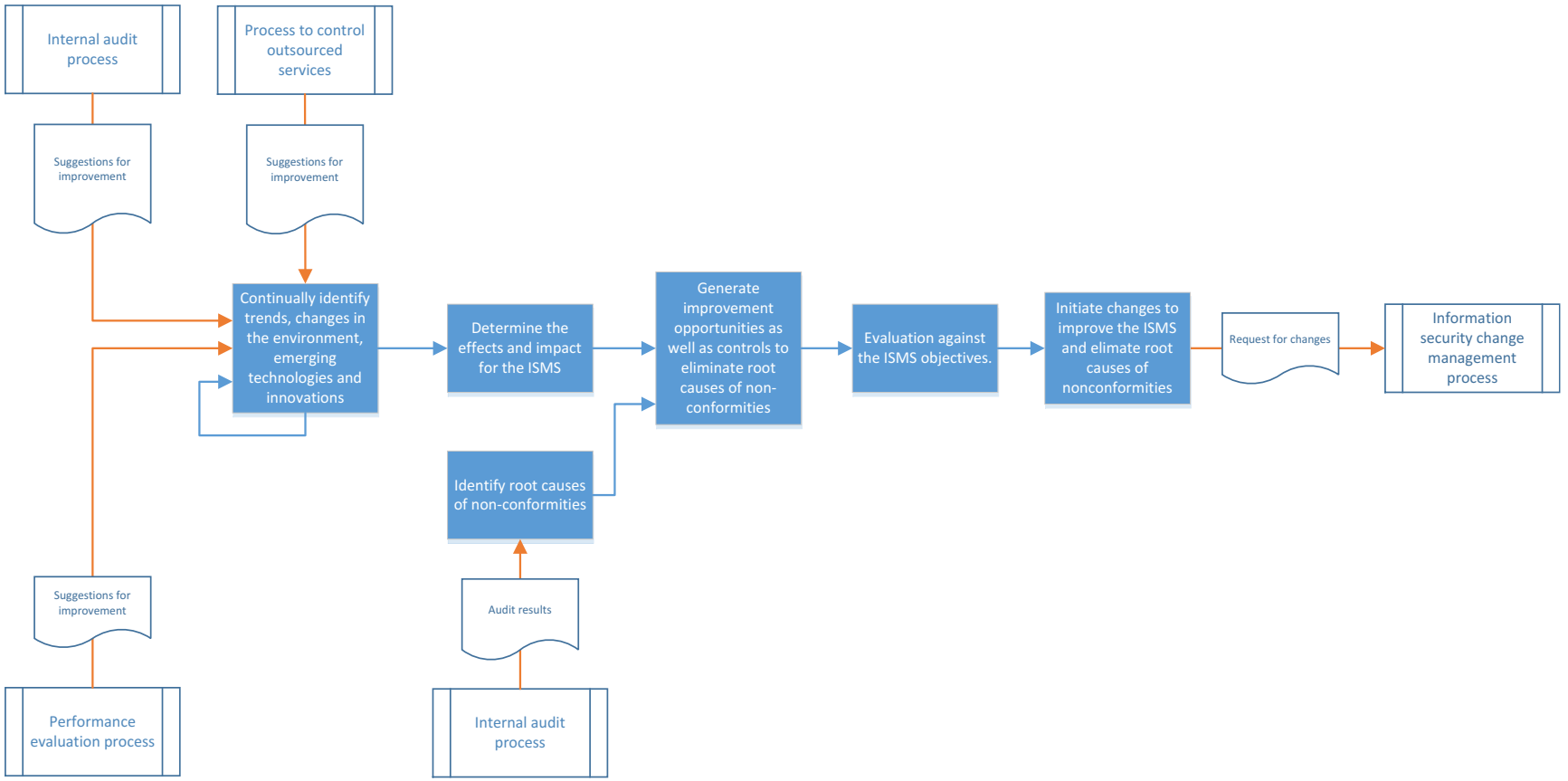

Figure 33 – Information security improvement process chart

Process Name	**Information security improvement process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (Information Systems Audit and Control Association, n.d.-c)**
Process category	ISMS core process
Brief description	The effectiveness, efficiency, suitability and adequacy of the ISMS need to be continually improved. A culture of continual improvement should be established. Emerging technologies and innovations also need to be identified and assessed regarding potential ISMS-improvement possibilities.
Objectives/purposes	Objective of this process is to ensure and improve a continuing suitability, adequacy and effectiveness of the ISMS.
Input	• From internal audit process: suggestions for improvement and audit reports • From process to control outsourced services: suggestions for improvement • From performance evaluation process: suggestions for improvement
Output	• For documentation and records control process: decisions related to continual improvement opportunities (not displayed in the process chart • For information security change management: change requests
Activities/functions	• Continually identify trends, changes in the environment, emerging technologies and innovations • Determine the effects and impact of trends, changes in the environment, emerging technologies and innovations for the ISMS • Identify root causes of non-conformities • Generate improvement opportunities as well as controls to eliminate root causes of non-conformities and evaluate them against the ISMS objectives. • Initiate changes to improve the ISMS
Metrics	• Count of eliminated root causes of non-conformities • Count of changes initiated by the information security improvement process
Owner	Information security officer
Manager	Information security officer
Actors	Internal auditors Information security officer

Table 69 – Information security improvement process

12.16 Information security customer relationship management process

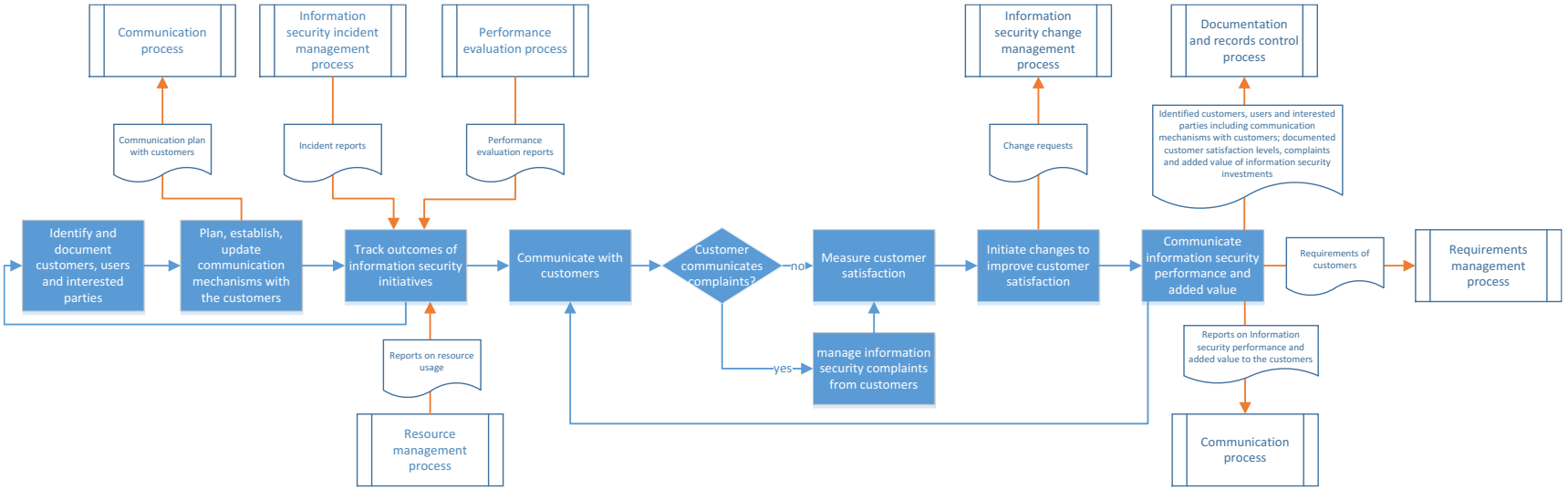

Figure 34 – Information security customer relationship management process

Process Name	**Information security customer relationship management process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (Information Systems Audit and Control Association, n.d.-c)**
Process category	ISMS core process
Brief description	This process enables the management of the customer satisfaction level as well as the continuous demonstration of the added value of investments in information security.
Objectives/purposes	• Ensure an appropriate balance between benefits, and costs of information security investments as well as risks • Ensure an appropriate customer satisfaction • Continuously demonstrate the added value of the ISMS or information security controls.
Input	• From performance evaluation process: performance evaluation reports • From resource management process: reports regarding the usage of resources • From incident management process: incident reports
Output	• For documentation and records control process: identified customers, users and interested parties including communication mechanisms with customers; documented customer satisfaction levels, complaints and added value of information security investments • For information security change management process: change requests • For communication process: information security performance and added value to the customers and communication mechanism (communication plan) with the customer • For requirements management process: requirements of customers
Activities/functions	• Identification and documentation of the customers, users and interested parties • Establishment of a communication mechanism with the customer • Establish a method for measuring and demonstrating the value of information security and the efficient resource usage(Information Systems Audit and Control Association, n.d.-c, p. 53). – Track outcomes of information security initiatives and compare to expectations to ensure value delivery against business goals. – Measurement of the customer satisfaction at planned intervals – Establish a documented procedure to manage

Process Name	Information security customer relationship management process – partially derived from (International Organization for Standardization and International Electrotechnical Commission, 2010a), (International Organization for Standardization and International Electrotechnical Commission, 2013), (International Organization for Standardization and International Electrotechnical Commission, 2013) and (Information Systems Audit and Control Association, n.d.-c)
	information security complaints from the customer • Initiation of changes to improve the customer satisfaction • Communicate information security performance and added value to the customers
Metrics	• Customer satisfaction level including trends • Count of complaints • Count of changes initiated by the information security customer relationship management
Owner	Information security officer
Manager	Information security officer
Actors	Internal auditors Information security officer

Table 70 – Information security customer relationship management process

13 Appendix C – Results of the ISMS core criteria study

#	company or public governance	Role	Named criteria							
			Repeatability / Regularity	Transformation of input into output	Defined responsibilities and accountabilities	Information security officer or manager is the process owner	Defined start and end of the process	Value generation	Essential for reaching the objectives of the organization	Process is operated in the ISMS
1	P	ISM	x	x						
2	C	ISO	x	x		x		x	x	
3	C	ISO	x	x		x		x		x
4	P	ISM	x	x	x		x			x
5	C	ISM	x	x	x	x				
6	C	Auditor	x	x	x		x	x	x	
7	C	Consultant	x	x		x		x	x	x
8	C	ISO				x		x	x	x
9	P	ISO	x	x	x		x	x		
10	C	ISO	x	x		x				x
11	C	ISM				x		x	x	
12	P	Auditor	x	x		x	x	x	x	x
13	P	ISO	x	x	x			x		
14	P	ISO			x	x	x	x	x	x
15	P	ISO	x			x		x	x	x
16	C	Consultant	x	x	x	x	x		x	x
17	P	ISO	x	x		x		x	x	x
18	P	ISO	x	x		x		x		x
19	P	ISO	x		x	x		x		x
20	P	ISO				x		x	x	x
21	P	ISO	x	x		x		x		
22	C	ISM	x	x		x	x	x		x
23	P	ISO								x
24	P	ISM				x		x		x
25	C	ISM	x	x		x		x	x	x
26	C	ISM	x	x	x		x			x
27	C	ISO	x			x		x	x	x
28	C	ISO	x					x		x
29	C	Auditor	x	x	x	x		x		x
30	P	Auditor				x		x		x
31	P	Auditor	x	x		x	x	x		x
32	C	Auditor	x	x	x	x	x	x		x
33	C	Auditor	x			x	x	x		x
34	C	Auditor	x	x	x	x	x	x		x
35	P	ISM	x			x		x		x
36	P	ISO			x	x		x	x	x
37	P	ISO	x	x		x	x			x
38	P	ISO	x	x		x	x			x
39	P	ISO	x			x	x	x		x
40	P	ISO				x		x		x
41	P	ISM	x		x	x		x		x
42	C	ISO	x			x		x		x
43	C	ISM	x	x		x		x	x	x
44	C	ISM			x		x			x
45	C	ISM	x			x		x		x
46	C	ISO	x		x	x		x		
47	C	ISM	x	x		x		x		x
48	C	ISM	x		x	x		x		x
49	P	ISO			x	x	x			x
50	P	ISO	x	x		x	x	x		
51	P	ISO	x			x				x
52	P	ISO			x		x	x	x	x
53	P	ISM	x	x		x				x
54	P	ISM						x		x
55	P	ISO	x		x	x	x	x		x
56	P	ISM	x	x		x		x		x
57	C	Auditor	x			x	x	x	x	
58	C	Auditor	x							x
59	C	Auditor	x	x	x	x	x	x		x
60	C	Auditor	x		x	x	x	x		x
61	C	Auditor	x	x	x	x		x	x	x
62	C	Auditor	x	x	x		x	x		x

#	company or public governance	Role	Named criteria							
			Repeatability / Regularity	Transformation of input into output	Defined responsibilities and accountabilities	Information security officer or manager is the process owner	Defined start and end of the process	Value generation	Essential for reaching the objectives of the organization	Process is operated in the ISMS
63	C	Consultant	x	x	x	x	x	x		x
64	C	Consultant		x		x	x	x		
65	C	Consultant	x		x	x		x		x
66	C	Consultant	x	x	x	x	x	x	x	x
67	C	Consultant	x	x	x	x	x	x		x
68	C	Consultant	x	x	x	x		x		x
69	C	ISM	x			x		x		x
70	C	ISO	x	x	x	x		x	x	x
71	C	ISM	x	x	x	x		x	x	x
72	C	ISO	x		x	x		x		x
73	P	ISO		x	x	x		x		x
74	P	ISO	x				x			
75	C	ISM	x	x	x	x		x	x	x
Sum	0	0	60	41	34	61	29	60	22	62

Table 71 – Results of ISMS core criteria study

14 Appendix D – Results of the ISMS core process study

Given were the following processes as well as the possibility to name additional processes:

#	Process/standard	Nr. in Table 73
1	ISMS planning process	1
2	Information security risk assessment process	2
3	Information security risk treatment process	3
4	Resource management process	4
5	Process to assure necessary awareness and competence	5
6	Communication process	6
7	Documentation control process	7
8	Requirements management process	8
9	Information security change management process	9
10	Process to control outsourced processes	10
11	Performance evaluation process	11
12	Internal audit process	12
13	Information security improvement process	13
14	Information security governance process	14
15	Information security incident management process	15
16	Service level management process	16
17	Service reporting process	17
18	Service continuity and availability management process	18
19	Budgeting and accounting for services process	19
20	Capacity management process	20
21	Business relationship management process	21
22	Supplier management process	22
23	Incident and service request management process	23
24	Problem management process	24
25	Configuration management process	25
26	Change management process	26
27	Release and deployment management process	27
28	Information security customer relationship management process	28
29	Controlling process	29
30	Human resources management process	30
31	Facility management process	31

Table 72 – Given processes in the ISMS core process study

Table 73 is containing the detailed results of the ISMS core process study.

#	company or public governance	Role	Decision if it is a ISMS core process																														
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	P	ISM		x	x	x	x				x	x	x	x	x		x													x			
2	C	ISO		x	x		x	x	x	x	x	x	x	x	x		x			x										x			
3	C	ISO		x	x		x		x		x	x	x	x	x		x			x										x			
4	P	ISM		x	x	x	x	x	x	x		x	x	x	x		x													x			
5	C	ISM		x	x		x				x	x	x	x	x	x	x									x	x			x			
6	C	Auditor		x	x	x	x				x	x		x		x	x													x			
7	C	Consultant		x		x	x	x	x		x	x	x	x	x	x	x			x							x			x			
8	C	ISO		x	x	x	x	x	x	x	x	x	x	x	x		x													x			
9	P	ISO		x	x		x		x	x	x	x	x	x	x		x			x							x			x			
10	C	ISO		x	x		x		x	x	x	x	x	x	x		x				x									x			
11	C	ISM		x	x	x	x	x	x		x	x	x	x	x		x			x		x								x			
12	P	Auditor		x	x		x	x	x	x	x	x	x	x	x		x													x			
13	P	ISO		x	x	x	x	x	x	x	x	x	x	x	x		x																
14	P	ISO		x	x		x	x	x	x	x	x	x	x	x		x			x										x			
15	P	ISO		x	x		x	x	x		x	x	x	x	x		x			x										x			
16	C	Consultant		x	x	x	x					x	x	x	x		x													x			
17	P	ISO		x	x	x	x		x		x	x	x	x	x	x	x										x			x			
18	P	ISO		x	x		x	x	x	x	x	x		x	x		x													x			
19	P	ISO		x	x	x	x		x	x	x	x	x	x	x	x	x			x										x			
20	P	ISO		x	x		x				x	x	x	x	x		x			x		x								x			
21	P	ISO		x	x	x	x	x	x		x	x	x	x	x		x									x	x			x			
22	C	ISM		x	x		x		x	x	x	x	x	x	x		x													x			
23	P	ISO		x	x		x	x	x	x	x	x	x	x	x		x			x										x			
24	P	ISM		x	x	x	x		x	x	x	x		x	x		x													x			
25	C	ISM		x	x		x		x		x	x	x	x	x		x										x			x			

#	company or public governance	Role	Decision if it is a ISMS core process																														
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
26	C	ISM		x	x	x	x	x	x		x	x	x	x	x		x													x			
27	C	ISO		x	x		x	x	x	x	x	x	x	x	x	x	x			x										x			
28	C	ISO		x	x		x				x	x	x	x	x		x													x			
29	C	Auditor		x	x	x	x		x		x	x	x	x	x		x					x								x			
30	P	Auditor		x	x	x	x		x		x	x	x	x	x		x			x										x			
31	P	Auditor		x	x	x	x	x	x	x	x	x	x	x	x		x			x										x			
32	C	Auditor		x	x	x	x					x		x	x		x																
33	C	Auditor		x	x		x	x	x			x	x	x	x		x													x			
34	C	Auditor		x	x		x	x	x	x	x	x	x	x	x	x	x										x			x			
35	P	ISM		x	x		x				x	x	x	x	x		x				x									x			
36	P	ISO		x	x		x				x	x	x	x	x		x			x										x			
37	P	ISO		x	x	x	x		x		x	x	x	x	x		x													x			
38	P	ISO		x	x		x				x	x		x	x		x													x			
39	P	ISO		x	x		x					x		x	x		x													x			
40	P	ISO		x	x	x	x	x	x	x	x	x	x	x	x		x			x										x			
41	P	ISM		x	x	x	x	x	x		x	x	x	x	x		x			x										x			
42	C	ISO		x	x	x	x		x	x	x	x	x	x	x		x			x										x			
43	C	ISM		x	x		x					x	x	x	x		x													x			
44	C	ISM		x	x	x	x		x		x	x	x	x	x		x													x			
45	C	ISM		x	x		x	x	x	x	x	x	x	x	x	x	x			x										x			
46	C	ISO		x	x		x				x	x	x	x	x	x	x			x		x				x	x			x			
47	C	ISM		x	x	x	x	x	x	x	x	x		x	x		x													x			
48	C	ISM		x	x		x		x	x	x	x	x	x	x		x										x			x			
49	P	ISO		x	x		x		x		x	x	x	x	x	x	x			x	x	x					x			x			
50	P	ISO		x	x	x	x	x				x	x	x	x		x													x			

#	company or public governance	Role	Decision if it is a ISMS core process																														
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
51	P	ISO		x	x		x	x	x	x		x	x	x	x		x													x			
52	P	ISO		x	x	x	x		x		x	x	x	x	x		x													x			
53	P	ISM		x	x	x	x				x	x	x	x	x	x	x			x										x			
54	P	ISM		x	x		x	x	x	x	x	x	x	x	x		x													x			
55	P	ISO		x	x		x		x		x	x	x	x	x		x			x										x			
56	P	ISM		x	x	x	x		x		x	x	x	x	x		x																
57	C	Auditor		x	x	x	x	x	x		x	x	x	x	x		x													x			
58	C	Auditor		x	x	x	x		x		x	x	x	x	x		x													x			
59	C	Auditor		x	x		x	x				x		x	x		x													x			
60	C	Auditor		x	x		x		x	x	x	x	x	x	x	x	x			x										x			
61	C	Auditor		x	x		x		x	x	x	x	x	x	x		x													x			
62	C	Auditor		x	x		x				x	x	x	x	x	x	x													x			
63	C	Consultant		x	x	x	x				x	x	x	x	x	x	x			x										x			
64	C	Consultant		x	x		x	x	x		x	x	x	x	x		x			x										x			
65	C	Consultant		x	x		x				x	x	x	x	x	x	x			x	x	x								x			
66	C	Consultant		x	x	x	x	x	x		x	x	x	x	x		x										x						
67	C	Consultant		x	x	x	x	x	x	x	x	x		x	x		x													x			
68	C	Consultant		x	x		x	x	x	x	x	x	x	x	x		x													x			
69	C	ISM		x	x		x				x	x	x	x	x	x	x			x							x			x			
70	C	ISO		x	x		x				x	x	x	x	x		x													x			
71	C	ISM		x	x	x	x		x	x		x	x	x	x		x													x			
72	C	ISO		x	x	x	x		x		x	x	x	x	x		x			x										x			
73	P	ISO		x	x		x	x	x	x	x	x	x	x	x	x	x			x										x			
74	P	ISO		x	x	x	x		x	x	x	x	x	x	x		x													x			
75	C	ISM		x	x		x		x		x	x	x	x	x	x	x			x										x			

#	company or public governance	Role	Decision if it is a ISMS core process																														
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Sum	0	0	0	75	74	35	75	31	54	30	65	75	66	75	74	18	75	0	0	30	4	6	0	0	0	3	12	0	0	71	0	0	0

Table 73 – Results of the ISMS core process study

15 Appendix E – Results of atomization of ISO 27001

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
1	Context of the Organisation	4.1	Understanding the organization and its context	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	ISMS planning process
2	Context of the Organisation	4.2	Understanding the needs and expectations of interested parties	The organization shall determine interested parties that are relevant to the information security management system.	ISMS planning process
3	Context of the Organisation	4.2	Understanding the needs and expectations of interested parties	The organization **shall determine the requirements of interested parties relevant to information security**.	Requirements management process
4	Context of the Organisation	4.3	Determining the scope of the information security management system	The organization shall determine the boundaries and applicability of the information security management system to establish its scope.	ISMS planning process
5	Context of the Organisation	4.3	Determining the scope of the information security management system	When determining this scope, the organization shall consider the external and internal issues referred to in 4.1.	Requirements management process
6	Context of the Organisation	4.3	Determining the scope of the information security management system	When determining this scope, the organization shall consider the requirements referred to in 4.2.	ISMS planning process
7	Context of the Organisation	4.3	Determining the scope of the information security management system	When determining this scope, the organization shall consider interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.	ISMS planning process
8	Context of the Organisation	4.4	Information security management system	The organization shall establish, implement, **maintain** and continually improve an information security management system, in accordance with the requirements of this International Standard.	ISMS planning process Information security incident management process

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
10	Leadership	5.1	Leadership and commitment	**Top management shall demonstrate leadership and commitment with respect to the information security management system by** ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization.	Information security governance process
11	Leadership	5.1	Leadership and commitment	Top management shall demonstrate leadership and commitment with respect to the information security management system by ensuring the integration of the information security management system requirements into the organization's processes.	Information security governance process
12	Leadership	5.1	Leadership and commitment	Top management shall demonstrate leadership and commitment with respect to the information security management system by ensuring that the **resources needed for the information security management system are available.**	Information security governance process Resource management process
13	Leadership	5.1	Leadership and commitment	Top management shall demonstrate leadership and commitment with respect to the information security management system by communicating the importance of effective information security management and of conforming to the information security management system requirements.	Information security governance process
14	Leadership	5.1	Leadership and commitment	Top management shall demonstrate leadership and commitment with respect to the information security management system by ensuring that the information security management system achieves its intended outcome(s).	Information security governance process
15	Leadership	5.1	Leadership and commitment	Top management shall demonstrate leadership and commitment with respect to the information security management system by directing and supporting persons to contribute to the effectiveness of the information security	Information security governance process

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
				management system.	
16	Leadership	5.1	Leadership and commitment	Top management shall demonstrate leadership and commitment with respect to the information security management system by promoting continual improvement.	Information security governance process
17	Leadership	5.1	Leadership and commitment	Top management shall demonstrate leadership and commitment with respect to the information security management system by supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	Information security governance process
18	Leadership	5.2	Policy	Top management shall establish an information security policy that is appropriate to the purpose of the organization.	Information security governance process
19	Leadership	5.2	Policy	Top management shall establish an information security policy that includes information security objectives (see 6.2) or provides the framework for setting information security objectives.	Information security governance process
20	Leadership	5.2	Policy	Top management shall establish an information security policy that includes a commitment to satisfy applicable requirements related to information security.	Information security governance process
21	Leadership	5.2	Policy	Top management shall establish an information security policy that includes a commitment to continual improvement of the information security management system.	Information security governance process
22	Leadership	5.2	Policy	The information security policy shall be available as documented information.	Documentation and records control process
23	Leadership	5.2	Policy	The information security policy shall be communicated within the organization.	Communication process
24	Leadership	5.2	Policy	The information security policy shall be available to interested parties, as appropriate.	Communication process
25	Leadership	5.3	Organizational roles,	Top management shall assign the responsibility and	Information security

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
			responsibilities and authorities	authority for ensuring that the information security management system conforms to the requirements of this International Standard.	governance process
26	Leadership	5.3	Organizational roles, responsibilities and authorities	Top management shall assign the responsibility and authority for reporting on the performance of the information security management system to top management.	Information security governance process
29	Planning	6.1.1	General actions to address risks and opportunities	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to ensure the information security management system can achieve its intended outcome(s).	ISMS planning process
30	Planning	6.1.1	General actions to address risks and opportunities	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and **determine the risks and opportunities that need to be addressed to prevent, or reduce, undesired effects.**	ISMS planning process Information security incident management process
31	Planning	6.1.1	General actions to address risks and opportunities	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to achieve continual improvement	ISMS planning process
32	Planning	6.1.1	General actions to address risks and opportunities	The organization shall plan actions to address these risks and opportunities.	ISMS planning process
33	Planning	6.1.1	General actions to address risks and opportunities	The organization shall plan how to integrate and implement the actions into its information security management system processes.	ISMS planning process
34	Planning	6.1.1	General actions to address risks and opportunities	The organization shall plan how to evaluate the effectiveness of these actions.	ISMS planning process

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
35	Planning	6.1.2	Information security risk assessment	The organization shall define and apply an information security risk assessment process that establishes and maintains information security risk criteria that include the risk acceptance criteria.	Information security risk assessment process
36	Planning	6.1.2	Information security risk assessment	The organization shall define and apply an information security risk assessment process that establishes and maintains information security risk criteria that include criteria for performing information security risk assessments.	Information security risk assessment process
37	Planning	6.1.2	Information security risk assessment	The organization shall define and apply an information security risk assessment process that ensures that repeated information security risk assessments produce consistent, valid and comparable results.	Information security risk assessment process
38	Planning	6.1.2	Information security risk assessment	The organization shall define and apply an information security risk assessment process that identifies the information security risks, apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system	Information security risk assessment process
39	Planning	6.1.2	Information security risk assessment	The organization shall define and apply an information security risk assessment process that identifies the information security risks and identify the risk owners.	Information security risk assessment process
40	Planning	6.1.2	Information security risk assessment	The organization shall define and apply an information security risk assessment process that analyses the information security risks and assess the potential consequences that would result if the risks identified in 6.1.2 were to materialize.	Information security risk assessment process
41	Planning	6.1.2	Information security risk assessment	The organization shall define and apply an information security risk assessment process that analyses the information security risks and assess the realistic likelihood	Information security risk assessment process

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
				of the occurrence of the risks identified in 6.1.2.	
42	Planning	6.1.2	Information security risk assessment	The organization shall define and apply an information security risk assessment process that analyses the information security risks and determine the levels of risk.	Information security risk assessment process
43	Planning	6.1.2	Information security risk assessment	**The organization shall define and apply an information security risk assessment process** that evaluates the information security risks and compare the results of risk analysis with the risk criteria established in 6.1.2.	Information security risk assessment process
44	Planning	6.1.2	Information security risk assessment	The organization shall define and apply an information security risk assessment process that evaluates the information security risks and prioritize the analysed risks for risk treatment.	Information security risk assessment process
45	Planning	6.1.2	Information security risk assessment	The organization shall retain documented information about the information security risk assessment process	Information security risk assessment process
46	Planning	6.1.3	Information security risk treatment	**The organization shall define and apply an information security risk treatment process** to select appropriate information security risk treatment options, taking account of the risk assessment results.	Information security risk treatment process
47	Planning	6.1.3	Information security risk treatment	The organization shall define and apply an information security risk treatment process to determine all controls that are necessary to implement the information security risk treatment option(s) chosen.	Information security risk treatment process
48	Planning	6.1.3	Information security risk treatment	The organization shall define and apply an information security risk treatment process to compare the controls determined in 6.1.3 above with those in Annex A and verify that no necessary controls have been omitted.	Information security risk treatment process
49	Planning	6.1.3	Information security risk treatment	The organization shall define and apply an information security risk treatment process to produce a Statement of Applicability that contains the necessary controls (see 6.1.3) and justification for inclusions, whether they are	Information security risk treatment process

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
				implemented or not, and the justification for exclusions of controls from Annex A.	
50	Planning	6.1.3	Information security risk treatment	The organization shall define and apply an information security risk treatment process to formulate an information security risk treatment plan.	Information security risk treatment process
51	Planning	6.1.3	Information security risk treatment	The organization shall define and apply an information security risk treatment process to obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	Information security risk treatment process
52	Planning	6.1.3	Information security risk treatment	The organization shall retain documented information about the information security risk treatment process.	Documentation and records control process
53	Planning	6.2	Information security objectives and planning to achieve them	The organization shall establish information security objectives at relevant functions and levels.	Information security governance process
54	Planning	6.2	Information security objectives and planning to achieve them	The information security objectives shall be consistent with the information security policy.	Information security governance process
55	Planning	6.2	Information security objectives and planning to achieve them	The information security objectives shall be measurable (if practicable).	Performance evaluation process
56	Planning	6.2	Information security objectives and planning to achieve them	The information security objectives shall take into account applicable information security requirements, and results from risk assessment and risk treatment.	Requirements management process
57	Planning	6.2	Information security objectives and planning to achieve them	The information security objectives shall be communicated.	Communication process
58	Planning	6.2	Information security objectives and planning to achieve them	The information security objectives shall be updated as appropriate.	Information security improvement process
59	Planning	6.2	Information security objectives and planning to achieve them	The organization shall retain documented information on the information security objectives.	Documentation and records control process
60	Planning	6.2	Information security objectives and planning to achieve them	When planning how to achieve its information security objectives, the organization shall determine what will be done.	Information security risk treatment process
61	Planning	6.2	Information security objectives and planning to achieve them	When planning how to achieve its information security objectives, the organization **shall determine what**	Resource management process

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
				resources will be required.	
62	Planning	6.2	Information security objectives and planning to achieve them	When planning how to achieve its information security objectives, the organization shall determine who will be responsible.	Information security governance process
63	Planning	6.2	Information security objectives and planning to achieve them	When planning how to achieve its information security objectives, the organization shall determine when it will be completed.	Information security governance process
64	Planning	6.2	Information security objectives and planning to achieve them	When planning how to achieve its information security objectives, the organization shall determine how the results will be evaluated.	Internal audit process
66	Support	7.1	Resources	The organization **shall determine and provide the resources** needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	Resource management process
67	Support	7.2	Competence	The organization **shall determine the necessary competence of person(s) doing work under its control that affects ist information security performance.**	Process to assure necessary awareness and competence
68	Support	7.2	Competence	The organization **shall ensure that these persons are competent on the basis of appropriate education, training, or experience.**	Process to assure necessary awareness and competence
69	Support	7.2	Competence	The organization shall where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken.	Performance evaluation process
70	Support	7.2	Competence	The organization shall retain appropriate documented information as evidence of competence.	Documentation and records control process
71	Support	7.3	Awareness	Persons doing work under the organization's control shall be aware of the information security policy.	Communication process
72	Support	7.3	Awareness	Persons doing work under the organization's control shall be aware of their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance.	Process to assure necessary awareness and competence

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
73	Support	7.3	Awareness	Persons doing work under the organization's control shall be aware of the implications of not conforming with the information security management system requirements.	Process to assure necessary awareness and competence
74	Support	7.4	Communication	**The organization shall determine the need for internal and external communications relevant to the information security management system including on what to communicate.**	Communication process
75	Support	7.4	Communication	**The organization shall determine the need for internal and external communications relevant to the information security management system including when to communicate.**	Communication process
76	Support	7.4	Communication	**The organization shall determine the need for internal and external communications relevant to the information security management system including with whom to communicate.**	Communication process
77	Support	7.4	Communication	**The organization shall determine the need for internal and external communications relevant to the information security management system including who shall communicate.**	Communication process
78	Support	7.4	Communication	**The organization shall determine the need for internal and external communications relevant to the information security management system including the processes by which communication shall be effected.**	Communication process
79	Support	7.5	Documented information	**The organization's information security management system shall include documented information required by this International Standard.**	Documentation and records control process
80	Support	7.5.1	General requirements regarding documented information	The organization's information security management system shall include documented information required by this International Standard. NOTE The extent of documented information for an information security management system can differ from	Documentation and records control process

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
				one organization to another due to: 1) the size of organization and its type of activities, processes, products and services; 2) the complexity of processes and their interactions; and 3) the competence of persons.	
82	Support	7.5.2	Creating and updating documented information	When creating and updating documented information the organization shall ensure appropriate identification and description (e.g. a title, date, author, or reference number).	Documentation and records control process
83	Support	7.5.2	Creating and updating documented information	When creating and updating documented information the organization shall ensure appropriate format (e.g. language, software version, graphics) and media (e.g. paper, electronic).	Documentation and records control process
84	Support	7.5.2	Creating and updating documented information	When creating and updating documented information the organization shall ensure appropriate review and approval for suitability and adequacy.	Documentation and records control process
85	Support	7.5.3	Control of documented information	Documented information required by the information security management system and by this International Standard shall be controlled to ensure it is available and suitable for use, where and when it is needed.	Documentation and records control process
86	Support	7.5.3	Control of documented information	Documented information required by the information security management system and by this International Standard shall be controlled to ensure it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).	Documentation and records control process
87	Support	7.5.3	Control of documented information	For the control of documented information, the organization shall address the following activities, as applicable distribution, access, retrieval and use.	Documentation and records control process
88	Support	7.5.3	Control of documented information	For the control of documented information, the organization shall address the following activities, as applicable storage and preservation, including the preservation of legibility.	Documentation and records control process

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
89	Support	7.5.3	Control of documented information	For the control of documented information, the organization shall address the following activities, as applicable control of changes (e.g. version control).	Information security change management process
90	Support	7.5.3	Control of documented information	For the control of documented information, the organization shall address the following activities, as applicable retention and disposition.	Documentation and records control process
91	Support	7.5.3	Control of documented information	Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.	Documentation and records control process
93	Operation	8.1	Operational planning and control	**The organization shall plan, implement and control the processes needed to meet information security requirements**, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.	Requirements management process Information security incident management process
94	Operation	8.1	Operational planning and control	The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.	Documentation and records control process
95	Operation	8.1	Operational planning and control	The organization **shall control planned changes and review the consequences of unintended changes,** taking action to mitigate any adverse effects, as necessary.	Information security change management process
96	Operation	8.1	Operational planning and control	The organization **shall ensure that outsourced processes are determined and controlled.**	Process to control outsourced services
97	Operation	8.2	Information security risk assessment	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2.	Information security risk assessment process
98	Operation	8.2	Information security risk assessment	The organization shall retain documented information of the results of the information security risk assessments.	Information security risk assessment process

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
99	Operation	8.3	Information security risk treatment	The organization shall implement the information security risk treatment plan.	Information security risk treatment process
100	Operation	8.3	Information security risk treatment	The organization shall retain documented information of the results of the information security risk treatment.	Information security risk treatment process
102	Performance Evaluation	9.1	Monitoring, measurement, analysis and evaluation	The **organization shall evaluate the information security performance and the effectiveness of the information security management system.**	Performance evaluation process Information security incident management process
103	Performance Evaluation	9.1	Monitoring, measurement, analysis and evaluation	**The organization shall determine what needs to be monitored** and measured, including information security processes and controls.	Performance evaluation process
104	Performance Evaluation	9.1	Monitoring, measurement, analysis and evaluation	The organization shall determine the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. NOTE The methods selected should produce comparable and reproducible results to be considered valid.	Performance evaluation process
105	Performance Evaluation	9.1	Monitoring, measurement, analysis and evaluation	The organization shall determine when the monitoring and measuring shall be performed.	Performance evaluation process
106	Performance Evaluation	9.1	Monitoring, measurement, analysis and evaluation	The organization shall determine who shall monitor and measure.	Performance evaluation process
107	Performance Evaluation	9.1	Monitoring, measurement, analysis and evaluation	The organization shall determine when the results from monitoring and measurement shall be analysed and evaluated.	Performance evaluation process
108	Performance Evaluation	9.1	Monitoring, measurement, analysis and evaluation	The organization shall determine who shall analyse and evaluate these results.	Performance evaluation process
109	Performance Evaluation	9.1	Monitoring, measurement, analysis and evaluation	The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.	Documentation and records control process

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
110	Performance Evaluation	9.2	Internal audit	**The organization shall conduct internal audits at planned intervals** to provide information on whether the information security management system conforms to the organization's own requirements for its information security management system.	Internal audit process
111	Performance Evaluation	9.2	Internal audit	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the requirements of this International Standard.	Internal audit process
112	Performance Evaluation	9.2	Internal audit	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to is effectively implemented and maintained.	Internal audit process
113	Performance Evaluation	9.2	Internal audit	The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits.	Internal audit process
114	Performance Evaluation	9.2	Internal audit	The organization shall define the audit criteria and scope for each audit.	Internal audit process
115	Performance Evaluation	9.2	Internal audit	The organization shall select auditors and conduct audits that ensure objectivity and the impartiality of the audit process.	Internal audit process
116	Performance Evaluation	9.2	Internal audit	The organization shall ensure that the results of the audits are reported to relevant management.	Communication process
117	Performance Evaluation	9.2	Internal audit	The organization shall retain documented information as evidence of the audit programme(s) and the audit results.	Documentation and records control process
118	Performance Evaluation	9.3	Management review	Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and	Information security governance process

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
				effectiveness.	
119	Performance Evaluation	9.3	Management review	The management review shall include consideration of the status of actions from previous management reviews.	Information security governance process
120	Performance Evaluation	9.3	Management review	The management review shall include consideration of changes in external and internal issues that are relevant to the information security management system.	Information security governance process
121	Performance Evaluation	9.3	Management review	The management review shall include consideration of feedback on the information security performance, including trends in nonconformities and corrective actions.	Information security governance process
122	Performance Evaluation	9.3	Management review	The management review shall include consideration of feedback on the information security performance, including trends in monitoring and measurement results.	Information security governance process
123	Performance Evaluation	9.3	Management review	The management review shall include consideration of feedback on the information security performance, including trends in audit results.	Information security governance process
124	Performance Evaluation	9.3	Management review	The management review shall include consideration of feedback on the information security performance, including trends in fulfilment of information security objectives.	Information security governance process
125	Performance Evaluation	9.3	Management review	The management review shall include consideration of feedback from interested parties.	Information security governance process
126	Performance Evaluation	9.3	Management review	The management review shall include consideration of results of risk assessment and status of risk treatment plan.	Information security governance process
127	Performance Evaluation	9.3	Management review	The management review shall include consideration of opportunities for continual improvement.	Information security governance process
128	Performance Evaluation	9.3	Management review	The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.	Information security governance process
12	Performance	9.3	Management review	The organization shall retain documented information as	Information security

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
9	Evaluation			evidence of the results of management reviews.	governance process
131	Improvement	10.1	Nonconformity and corrective action	When a nonconformity occurs, the organization shall react to the nonconformity, and as applicable take action to control and correct it.	Information security improvement process
132	Improvement	10.1	Nonconformity and corrective action	When a nonconformity occurs, the organization shall react to the nonconformity, and as applicable deal with the consequences	Information security improvement process
133	Improvement	10.1	Nonconformity and corrective action	When a nonconformity occurs, the organization shall evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by reviewing the nonconformity.	Information security improvement process
134	Improvement	10.1	Nonconformity and corrective action	When a nonconformity occurs, the organization shall evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by determining the causes of the nonconformity.	Information security improvement process
135	Improvement	10.1	Nonconformity and corrective action	When a nonconformity occurs, the organization shall evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by determining if similar nonconformities exist, or could potentially occur.	Information security improvement process
136	Improvement	10.1	Nonconformity and corrective action	When a nonconformity occurs, the organization shall implement any action needed.	Information security improvement process
137	Improvement	10.1	Nonconformity and corrective action	When a nonconformity occurs, the organization shall review the effectiveness of any corrective action taken.	Information security improvement process
138	Improvement	10.1	Nonconformity and corrective action	When a nonconformity occurs, the organization shall make changes to the information security management system, if necessary.	Information security improvement process
139	Improvement	10.1	Nonconformity and corrective action	Corrective actions shall be appropriate to the effects of the nonconformities encountered.	Information security improvement process
14	Improvement	10.1	Nonconformity and corrective	The organization shall retain documented information as	Information security

#	Phase/Topic	Chapter	Chapter title	Content	Requirement is linked to which ISMS-Process?
0			action	evidence of the nature of the nonconformities and any subsequent actions taken.	improvement process
141	Improvement	10.1	Nonconformity and corrective action	The organization shall retain documented information as evidence of the results of any corrective action.	Information security improvement process
142	Improvement	10.2	Continual improvement	**The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.**	Information security improvement process

Table 74 – Atomized ISO 27001 requirements

16 Appendix F – Review protocol for the SLR regarding ISMS process framework

According to Kitchenham (B. Kitchenham, 2004) a review protocol specifies the methods that will be used to undertake the specific systematic review and consists of the following:

Background and research question

The rationale for conducting the review is, that the researcher want to answer the Research question MRQ-1 "Of which elements does the agreed ISMS core process framework consists?" – which is at the same time the objective of the review – and no primary study could be found regarding this research question.

Strategy to identify possible primary studies

To identify if any existing SLR regarding ISMS processes are available the following databases were searched with the search strings "SLR" AND "ISMS" as well as "Review" and "ISMS":

- IEEE
- ACM
- Science direct

Study selection criteria and procedures

The following selection criteria of the results were defined by the author of this thesis:

- Inclusion criteria – IC1: Any study/paper which is relevant for the research question
- Exclusion criteria – EC1: The title or abstract of the paper or study must include "ISMS" AND "Review" OR "SLR". If this is not the case, the paper will be excluded.
- Exclusion criteria – EC2: Paper or study which is not available in English or German

The criteria IC1 and EC1 will be applied in one step. For this the research results will be sorted according to the relevance using the algorithms of the searched databases. Titles and abstracts will be read to check if the key words of EC1 are present in the abstract or the title.

Additionally abstracts and titles will be read to check, if any hint is included that the paper contains a relevant SLR without using the identified key words. This would override EC1.

The last step is to exclude any paper or study which is not available in English or German. This is also checked while reading the abstracts/titles.

To avoid unnecessary efforts in this early stage of the SLR the assessment of the IC and ECs will be stopped, when a series of consecutive papers or studies (ten percent of the results, but at least ten papers) were excluded from the by relevance sorted result lists of the searched databases.

The evaluation of the inclusion and exclusion criteria will be performed by the author of this thesis.

Study quality assessment checklists and procedures

Obsolete as no relevant study was identified.

Data extraction strategy

Obsolete as no relevant study was identified.

Synthesis of the extracted data

Obsolete as no relevant study was identified.

Project timetable

SLR phase	Intended period
Planning the review	***February 2016***
Conducting the review	***March – April 2016***
Reporting the review	***May 2016***

Table 75 – Project timetable SLR ISMS processes

Protocol review

This protocol was presented to the supervisors Ricardo Colomo-Palacios and Vladimir Stantchev for review and criticism and was agreed before conducting the review.

17 Appendix G – Review protocol for the SLR regarding the usage of maturity level models within an ISMS

According to Kitchenham (2004) a review protocol specifies the methods that will be used to undertake the specific systematic review and consists of the following:

Background and research question

The rationale for conducting the review is, that the researcher want to answer the Research question MRQ2-2 "Are maturity models already used within ISMS?" – which is at the same time the objective of the review – and no primary study could be found regarding this research question.

Strategy to identify possible primary studies

To identify if any existing SLR regarding ISMS processes are available the following databases were searched with the search ("SLR" AND "ISMS" AND "Maturity"):

- IEEE
- ACM
- Science direct

Study selection criteria and procedures

The following selection criteria of the results were defined by the author of this thesis:

- Inclusion criteria – IC1: Any study/paper which is relevant for the research question
- Exclusion criteria – EC1: The title or abstract of the paper or study must include "ISMS" AND "Maturity" AND "SLR". If this is not the case, the paper will be excluded.
- Exclusion criteria – EC2: Paper or study which is not available in English or German

The criteria IC1 and EC1 will be applied in one step. For this the research results will be sorted according to the relevance using the algorithms of the searched databases. Titles and abstracts will be read to check if the key words of EC1 are present in the abstract or the title.

Additionally abstracts and titles will be read to check, if any hint is included that the paper contains a relevant SLR without using the identified key words. This would override EC1.

The last step is to exclude any paper or study which is not available in English or German. This is also checked while reading the abstracts/titles.

To avoid unnecessary efforts in this early stage of the SLR the assessment of the IC and ECs will be stopped, when a series of consecutive papers or studies (ten percent of the results, but at least ten papers) were excluded from the by relevance sorted result lists of the searched databases.

The evaluation of the inclusion and exclusion criteria will be performed by the author of this thesis.

Study quality assessment checklists and procedures

Obsolete as no relevant study was identified.

Data extraction strategy

Obsolete as no relevant study was identified.

Synthesis of the extracted data

Obsolete as no relevant study was identified.

Project timetable

SLR phase	Intended period
Planning the review	***February 2016***
Conducting the review	***March – April 2016***
Reporting the review	***May 2016***

Table 76 – Project timetable SLR ISMS maturity level model

Protocol review

This protocol was presented to the directores Ricardo Colomo-Palacios and Vladimir Stantchev for review and criticism and was agreed before conducting the review.

18 Appendix H – Pilot application – Target process maturity analysis – Process to control outsourced services

The following table contains the answers to the questionnaire regarding the target process maturity level for the process to control outsourced services.

The answers were obtained in a workshop with the information security officer as well as representative staff carrying out the process.

Criteria Questions regarding the organization – to be answered only once for an organization	Questions	answers
Organizations objectives and vision	What are the objectives and the vision of the organization?	The main objective of the organization is to provide a reliable and secure infrastructure which is used by several government organization.
Industry classification	What is the industry classification of the organization? For example: • Capital-intensive industries, other than utilities (Cap) • Utilities (Util) • Service industries (Srv) • Financial institutions (Fin) • Government and non-profits (Govt)	Government
Size of IT operations	What is the size of IT operations taking into account: • IT staff members • Application systems • Clients?	The IT staff consists of about ten persons. The provision of the office infrastructures (clients, printer, email- and internet services) are outsourced to another government organization.
Maturity level of core business processes	What is the maturity level of the core business processes?	The maturity of the business processes could be best described between maturity level 2 and 3. The government organization is comparatively young. So process maturity is atypically low compared to other government organizations. But as most staff of the organizations is newly recruited, process maturity is

Criteria	Questions	answers
		also improving comparatively fast (also atypical for government organizations).
General process specific questions		
Current maturity level of the process	What is the current maturity level of the process?	3
Complexity of the process	How complex is the process? How many decisions and alternative paths does the process contain?	The actual process can be described as complex as the outsourced processes are crucial to reach the objective of the organization. This process is atypically complex and linked to the change management process (as changes to the contract occur regularly and the contract itself is complex) as well as linked with the information security incident management process (dealing with incidents from the service provider).
Degree of visibility of the process and/or process results	How visible is the process and the process results to - Stakeholders of the process? - the public?	Process results are highly visible as the outsourced processes are crucial to reach the objective of the organization.
Questions regarding process performance objectives		
Importance of process result quality	How important is the quality of the process results?	The quality of the process results are highly important as the outsourced processes are crucial to reach the objective of the organization. 5 importance points
Importance of processing speed	How important is a processing time?	Speed must be sufficient to ensure the necessary quality of the provided services. For example long processing time for contract changes does not enable the service provider to provide the right and necessary services at the necessary quality level. 3 importance points
Importance of process flexibility	How necessary is it to ensure a flexibility of process steps?	Process flexibility is not important compared to process

Criteria	Questions	answers
	What degree of flexibility is needed?	result quality and processing speed. 1 importance point
Importance of process costs	How important is it to ensure minimum costs of process operation?	Costs of process operation are not important compared to process result quality and processing speed. 1 importance point
Dependability	How does the performance objectives of the process relate to the organizations objectives and vision? Which objectives and vision are influenced by the process and/or process results?	The organizations objectives are highly dependent on the services provided by the service provider. 5 importance points because the "strong dependency"
Questions regarding process output and costs		
Variation in demand of the process outputs	Are there specific points in time were process outputs are critical for other processes and/or for reaching organizations objectives and vision?	There is usually no variation in the demand of the process outputs.
Volume of the process output	What is the volume of the process output?	The volume of the process output cannot be described as high, but it is constant.
Variety of the process output	How many different process outputs do exist? How great is the variety of the process output?	Process output can vary significantly.
Costs	How much in terms of money, and work time does one process execution cost?	As process execution costs are not important, no reliable information is present about that.
Frequency of process operation	How often is the process operated?	The process is operated more or less continuously.
Consequences of changing current maturity level		
Costs / Benefits of specific maturity levels of the process	What are the costs to increase the maturity level (for each maturity level left)?	As already stated, costs are not important.
Costs / Benefits of specific maturity levels of the process	What are the benefits to increase the maturity level (for each maturity level left)?	Benefits of increasing the process maturity to level 4 would be significant. Taking into account the dependability from

Criteria	Questions	answers
		the process results a predictable process would be of great value. An innovating process seems not necessary as changes to the objectives of the organization occur very seldom.
Costs / Benefits of specific maturity levels of the process	What are the costs to decrease the maturity level (for each maturity level left)?	As already stated, costs are not important.
Costs / Benefits of specific maturity levels of the process	What are the benefits to decrease the maturity level (for each maturity level left)?	Taking into account the dependability from the process results a decrease of the process maturity is out of discussion.
Risks	What are the risks to operate the process at specific levels?	Because of the strong dependency and high quality requirements risks to operate the process at lower maturity levels than 4 are simply not reaching the main objectives of the organization.
Already communicated or identified requirements regarding the process (dependent also from the industry classification of the organization)		
Legal requirements	Are there specific legal requirements regarding the process or the process results (for example records of the process)?	Objectives of the organization are defined by law which influence the necessary process maturity.
Customer requirements	Are there requirements of customers to operate the process at a specific maturity level? If so: Which maturity level is stipulated by the customers?	Major requirements of the customers are a reliable and secure infrastructure which also influences the organizations and process objectives.
Management requirements	Are there requirements of the management to operate the process at a specific maturity level? If so: Which maturity level is stipulated by the management?	See customer requirements.

Table 77 – Target process maturity questionnaire – Process to control outsourced services

The result of the answers to the questionnaire regarding the target process maturity level for the process to control outsourced services the importance of the process performance

objectives were analyzed and shown in Figure 35 – Importance of process performance objectives – process to control outsourced services.

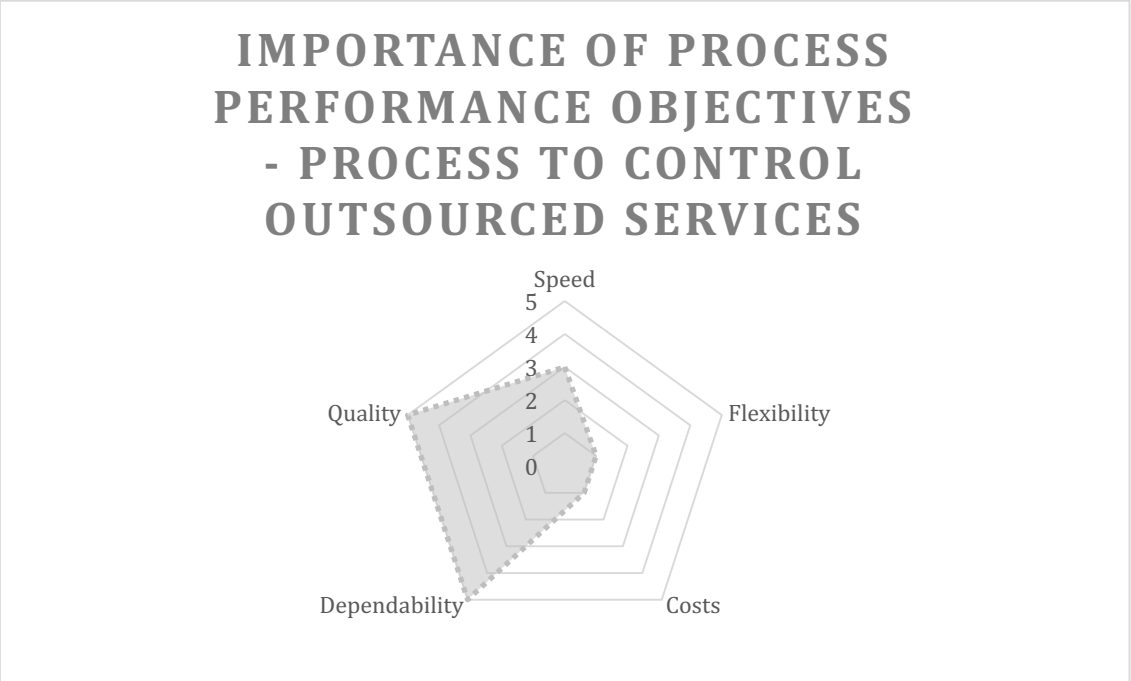

Figure 35 – Importance of process performance objectives – process to control outsourced services

As a result of the analysis of the answers to the questionnaire and a discussion of that answers with the information security officer as well as the management of the organization it was decided to increase the maturity level of that process to level 4.

19 Appendix I – Evaluation of the ISMS process framework against ISO 33004

This appendix is intended to discuss if the developed framework is a process reference model meeting the criteria defined in ISO/IEC 33004 (*Information technology -- Process assessment -- Requirements for process reference, process assessment and maturity models*, 2015) for process reference models.

According to *Information technology -- Process assessment -- Requirements for process reference, process assessment and maturity models* (2015) "The purpose of a process reference model is to define a set of processes that collectively can support the primary aims of a community of interest. A process reference model provides the basis for one or more process assessment models."

Criteria for process reference models defined in ISO/IEC 33004 are the following:

1) A process reference model shall contain a declaration of the domain of the process reference model.

   The proposed ISMS core process model is clearly dedicated to the use within information security risk management, which is a domain according to (Dubois, Heymans, Mayer, & Matulevičius, 2010)

2) A process reference model shall contain a description of the relationship between the process reference model and its intended context of use.

   As already stated earlier, the processes of the ISMS core process framework are formulated in a general manner to fit for all organizations independent of their size, objectives, business model, location et cetera. The ISMS core process framework shall be used in the context of a method to determine the necessary maturity level for each process contained in the framework. ISMS processes of the framework shall be tailored to the specific needs of the applying organization, and must be used only as a starting point. A general focus on a process perspective rather than a measure perspective is intended. A measurement driven approach, like the understanding of information security as a one-time project, shall be avoided and replaced by a process oriented approach.

3) A process reference model shall contain process descriptions, meeting the following requirements within the scope of the process reference model:

   a) A process shall be described in terms of its purpose and process outcomes.

      process purpose and outcomes are described within the process profiles of Appendix B – Process Profiles

   b) The described set of process outcomes shall be necessary and sufficient to achieve the purpose of the process

      The sets of process outcomes were defined with the intention to be necessary and sufficient for the purpose of the process. Every process purpose and the process outcome set were validated to be necessary and sufficient within a pilot application.

   c) Process descriptions shall not contain or imply aspects of the process quality characteristic beyond the basic level of any relevant process measurement framework conformant with ISO/IEC 33003.

      Every process was designed and defined with that rule in mind. So the resulting process description (see Appendix B – Process Profiles) do meet this requirement.

   d) A process outcome describes one of the following: production of an artifact; a significant change of state; meeting of specified constraints, e.g. requirements, goals etc.

      Every process outcome defined within the proposed ISMS core process framework meets this requirement (see Appendix B – Process Profiles).

   In general guidelines of ISO/IEC/TR 24774 (International Organization for Standardization and International Electrotechnical Commission, 2010) were considered while defining and describing the ISMS core processes.

4) A process reference model shall contain a description of the relationship between the processes defined within the process reference model.

   A description of the relationships between the processes are described within the process profiles (see Appendix B – Process Profiles). For every process input/output it is defined from which process it comes or in which process it will be further used.

5) The process reference model shall document the community of interest of the model and the actions taken to achieve consensus within that community of interest:

   a) The relevant community of interest shall be characterized or specified.

      The community of interest is every person accountable or responsible (partially or overall) for the management of information security risks. Also experts assessing an ISMS against ISO/IEC 27001 are included in the relevant community.

The extent of achievement of consensus shall be documented. If no actions are taken to are taken to achieve consensus, a statement to this effect shall be documented. documented.

Consensus regarding the processes itself were reached within an extensive expert expert consultation with experts of the community of interest. This is described in chapter described in chapter 0 “

b) Verification of the elements of the framework". Consensus regarding the elements of the processes described in the process descriptions was not verified within an expert consultation. Nevertheless consensus can be assumed taking into account that all processes were derived from internationally accepted standards.

6) The processes defined within a process reference model shall have unique process descriptions and identification.

   Every process has unique process descriptions and identification – (see Appendix B – Process Profiles)

As a result of the discussion above the framework proposed in this thesis meets the requirements for process reference models defined in ISO/IEC 33004. So, the proposed ISMS core process framework is a process reference model.