International Journal of Information Systems and Project Management

Volume 4 | Number 4 Article 3

2016

A process framework for information security management

Knut Haufe
Persicon Corporation

Ricardo Colomo-Palacios
Østfold University College

Srdan Dzombeta
Persicon Corporation

Knud Brandis
Persicon Corporation

International Journal of
Information Systems and Project Management
ISSN (print):2182-7796, ISSN (online):2182-7788, ISSN (cd-rom):2182-780X
Available online at www.sciencesphere.org/ijispm

A process framework for information security management

Knut Haufe
Persicon Corporation
Friedrichstraße 100, Berlin 10117, Germany
www.shortbio.net/khaufe@persicon.com

Knud Brandis
Persicon Corporation
Friedrichstraße 100, Berlin 10117, Germany
www.shortbio.net/kbrandis@persicon.com

Ricardo Colomo-Palacios
Østfold University College
B R A Veien 4, Halden 178, Norway
www.shortbio.net/ricardo.colomo-palacios@hiof.no

Vladimir Stantchev
SRH Hochschule Berlin
Ernst-Reuter-Platz 10, Berlin 10587, Germany
www.shortbio.net/vladimir.stantchev@srh-hochschule-berlin.de

Srdan Dzombeta
Persicon Corporation
Friedrichstraße 100, Berlin 10117, Germany
www.shortbio.net/sdzombeta@persicon.com

Abstract:
Securing sensitive organizational data has become increasingly vital to organizations. An Information Security Management System (ISMS) is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security. Key elements of the operation of an ISMS are ISMS processes. However, and in spite of its importance, an ISMS process framework with a description of ISMS processes and their interaction as well as the interaction with other management processes is not available in the literature. Cost benefit analysis of information security investments regarding single measures protecting information and ISMS processes are not in the focus of current research, mostly focused on economics. This article aims to fill this research gap by proposing such an ISMS process framework as the main contribution. It is based on a set of agreed upon ISMS processes in existing 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, as a main finding, the systemic character of the ISMS consisting of processes and the perception of relevant roles of the ISMS is strengthened.

Keywords:
information security; IT security management; ISMS; process framework.

DOI: 10.12821/ijispm040402

Manuscript received: 15 May 2016
Manuscript accepted: 30 August 2016

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 [1]. Information security is also identified as a subset of Information Technology (IT) governance [2]. In relevant standards and frameworks as well as in the scientific literature, the continuously increasing dependency of nearly all organizations on appropriate secure information processing was stated practically in the last years [3]–[5]. Standards for the management of information security and collections of best practice measures were developed and established in the literature, e.g. [6]. Important standards for the development and operation of an ISMS (hereinafter referred to as "ISMS") are the ISO 27000 series.

Over the last few years, cost benefit discussions have influenced information security practice [7]. The value of information must justify protection costs. Adjustment and cost-effectiveness are key elements of a successful ISMS [1]. Knowledge of the mission is needed to align the ISMS processes to the organization and its mission [8].

Taking into account that business alignment and cost-effectiveness 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 ISMS processes as core elements of every ISMS.

IT and its management are also some of the hot topics for practitioners and researchers alike [9]–[11]. In a scenario, in which security management has also been pointed out as one of the most important topics in the discipline, there is no specific process framework for security management which clearly differentiates between ISMS processes and of the security measures controlled by ISMS-processes. Furthermore, a detailed description of ISMS processes and their interaction as well as the interaction with other management processes – as already identified in [12] – does not exist.

This problem is further exasperated because information security management is a complex issue [13]. Current research activities focus on economics and cost benefit analysis of information security investment regarding single measures protecting information. The ISMS and the ISMS processes themselves are not in the focus of current research [14]–[16]. So, such a holistic but detailed framework of ISMS core processes as core elements of every ISMS needs to be developed.

This specific process framework for security management needs to clearly differentiate between ISMS core processes, supporting processes and management processes, as well as the security measures controlled by ISMS-processes. Adjustment and cost-effectiveness are key elements of a successful ISMS [1]. A detailed framework of ISMS processes (input, output, interfaces) and their interaction at an activity level help to ensure an appropriate interaction of the ISMS processes. To fill this research gap, in this paper a holistic but detailed framework of ISMS core processes as core elements of every ISMS is proposed.

The remaining of this paper is structured as follows: in section 2 authors give an overview of the most relevant standards on the topic. In section 3 authors describe the applied research methods and in section 4 authors illustrate the proposed ISMS process framework and discuss the contained processes. Section 5 gives an overview of the results from the evaluation of the framework. Section 6 summarizes the main findings and gives an outlook on future research activities.

2. Background

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 [17]–[19]. Standards for the management of information security and collections of best practice measures were developed and established [5], [20]–[22]. Beside national standards like NIST SP 800 series in the US [23] or the IT security guidelines from the Federal Office for Information security in Germany [22], the most important standards for the development and operation of an ISMS are

the ISO 270xx, ITIL and COBIT [24]. The same standards were identified in an ISACA study [25, p. 26] as most used standards for IT governance and IT management, followed by CMM and CMMI, PRINCE2 and PMBOK.

2.1 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 ISMSs. 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 [20], [26].

ISO 27001 contains the requirements for planning, implementing, operating, and improving an ISMS. 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 [27] but the standard contains requirements for ISMS core process. Therefore, this standard forms the basis to identify ISMS core processes.

The ISO 27000 series do not only contain ISO 27001. Another common standard for information security of the ISO 27000 series is ISO 27002 [21], 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 – ISMS 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.

2.2 ITIL

The IT Infrastructure Library (ITIL), specified in [28]–[33], 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 [34]. The primary objective of service management is to ensure that IT services are aligned to the business needs and actively support them [28]. 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 [32] – 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 [28] – 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 [33] – contains information about the development and improvement of capabilities regarding the implementation of new or changed services into production;
- Service Operation [31] – is focusing on the operation of IT services regarding efficiency and effectiveness;
- Continual Service Improvement [29] – contains instructions for the recurring improvement of design, implementation and operation of IT services (continual improvement process).

ISO/IEC 20000 [35], [36] 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 [28].

2.3 COBIT

Control Objectives for Information and related Technology (COBIT), specified in [37]–[40] is a control framework to help an organization ensure alignment between use of information technology and its business goals [41]. COBIT is based on five key principles [37]: Meeting stakeholder needs; Covering enterprise end-to-end; Applying a single, integrated framework; Enabling holistic approach; 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. COBIT will be analyzed with the aim to use or adapt the process reference model for the use with ISMS core processes. Furthermore a COBIT 5 Professional Guide for Information Security [40] 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 [42], [43]. In this article, the COBIT family is used to identify ISMS core processes and to integrate maturity levels in the ISMS core process framework.

3. Research methods

According to Susanto et al. [44] the most important and most widely accepted international initiatives for the development and operation of an ISMS are ISO 27000 series, ITIL [28]–[33] and COBIT [38]. These initiatives are also relevant in aspects like information and security management [10]. To obtain an agreed basis of ISMS processes of these standards, multiple process reference models need to be harmonized. To harmonize multiple process reference models a systematic stepwise approach presented by Baldassarre [45] was used in a mapping study by Haufe et al. [46]. For the analysis of the identified security management standards, an adaptation on the Models and Standards Similarity Study method by J. A. Calvo-Manzano et al. [47] was used. The method was as follows:

1. Select the models and standards to be analyzed;
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;
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 level of detail is chosen to analyze the standards;
5. Create a correspondence template – instead of a detailed correspondence template a process profile template was created;
6. Identify the similarity among models – the process templates were completed with information obtained from the standards;
7. Show obtained results.

Also the following basic criteria for ISMS core processes were identified and confirmed in a previous study [48] by the authors:

- Criteria 1 – Regularity – interrelated and interacting tasks are repeated on a regular basis;
- Criteria 2 – Transformation – inputs are transformed into outputs;
- Criteria 3 – Operationally – process is carried out while operating the ISMS;
- Criteria 4 – Accountability/responsibility – information security officer is the process owner or process manager and the process is a core competency of the ISMS;
- Criteria 5 – Value generating – delivers apparent and direct value to the stakeholder.

For the identification of processes, the following method was used:

1. Initially the ISO 27000 series were analyzed regarding mentioned processes;
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. A matching table regarding the possible ISMS processes was created for ITIL and COBIT [46]. In the context of the matching the following questions were asked (based on Calvo-Manzano et al. [47]):
    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?
3. The results from steps one and two were summarized in a mapping table which is documented in Haufe et al. [46].

The detailed approach of the mapping study is also described in Haufe et al. [46].

4. Process Framework

As a result of the mapping study the following processes were identified as ISMS processes:

Table 1. ISMS processes

Process/criteria	**Process category**
Process/criteria	Process category
ISMS planning process	Management process
Information security governance process	Management process
Information security risk assessment process	ISMS core process
Information security risk treatment process	ISMS core process
Resource management process	ISMS core process
Process to assure necessary awareness and competence	ISMS core process
Communication process	ISMS core process
Documentation and records control process	ISMS core process
Requirements management process	ISMS core process
Information security change management process	ISMS core process
Process to control outsourced processes	ISMS core process
Performance evaluation process	ISMS core process
Internal audit process	ISMS core process
Information security incident management process	ISMS core process
Information security improvement process	ISMS core process
Information security customer relationship management process	ISMS core process
Configuration management process	Support process

ISMS processes and their interaction at a high level basis are shown in Fig. 1. ISMS process framework. Some interfaces are not illustrated to enable a better readability of Fig. 1. ISMS process framework: Every ISMS process provides input for the documentation and records control process; The ISMS planning as well as the configuration management process provide input for every ISMS process.

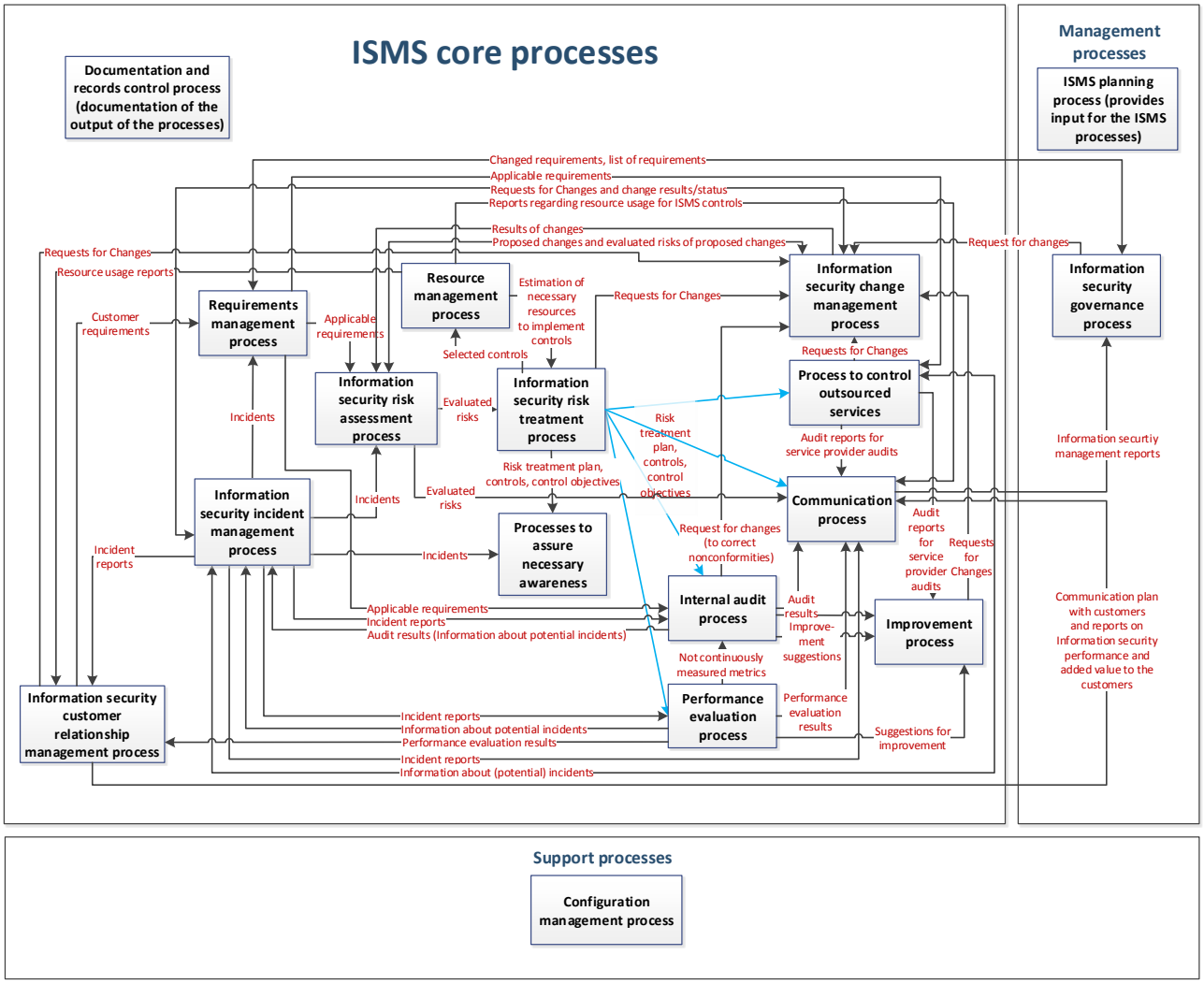


Fig. 1. ISMS process framework

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.

Resources needed to implement the controls as well as to run the ISMS processes 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 always results in 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. Output 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.

In the **information security awareness process** an information security awareness, training and education program is developed and implemented to ensure that all personnel receive 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.

Beside the information security governance process, which forms the interface between the ISMS and its stakeholders, the operational management of the customer satisfaction level as well as the continuous demonstration of the added

value of investments in information security need to be realized. This is done within the **information security customer relationship management process.**

The ISMS processes are discussed in more detail in the following subsections.

4.1 ISMS planning process

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. Some of the outputs of this process – like management approval, scope definition – need to be checked in a regular basis regarding their actuality and appropriateness, but the process itself is primary an initial process which is carried out once as a project [49, p. 5]. The regular activities like renewing the management approval are also integrated in the management review and improvement processes. The ISMS planning process is clearly a process of the plan phase in the Plan Do Check Act (PDCA) cycle which means that the process is not carried out while operating the ISMS (DO phase).

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

4.2 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 [50]. The management should initiate management reviews to continually improve the suitability, adequateness and effectiveness of the ISMS [20, 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.

Inputs like management reports are transformed into decisions related to the governance of the ISMS and related change requests.

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. However, the owner of this process is the top management, as top managers are responsible to initiate the review process and to provide objectives and requirements to manage the ISMS. Information security governance process objectives for the ISMS are defined and the achievement of the information security objectives are monitored at a general level. However, top managers review and decide relevant aspects on this process.

Results of this process like informed and efficient management decisions represent a direct value for the top management (stakeholders) as they ensure that the ISMS is operated as intended by the top management and will achieve their objectives as top managers. As a result of this this process is a core competence for top managers.

Given the fact that this process is not a core competence of the ISMS and 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. The integration of an ISMS with a service management system enables synergy effects based on the integration of these two processes.

4.3 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 [51, pp. 22–23]. Several iterations of this process are often conducted [51, pp. 9–10]. Inputs from ISMS planning process, information assets and previous process results are transformed into documented and evaluated risks and risk owners. 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 [51, p. 3]. The information security risk assessment process is a source of value for the top management while it provides a set of documented risks as well as a documented evaluation of those risks to help the decision making.

Again, this process is also part of the service management system [35, pp. 18–19]. One more time, synergy effects appear when the integration of ISMS and service management is made possible.

4.4 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 part of the risk management process, it should be monitored, reviewed and repeated regularly [51, p. 4].

In the information security risk treatment process, documented and evaluated risks are transformed into a risk treatment plan. 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 [51, p. 3].

The information security risk treatment process is value generating for the top management while it provides a documented risk treatment plan.

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 not objectives the organization. So, it has an operational character.

4.5 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. A resource management process is also part of the ISMS planning process. This process focusses on the resources necessary to operationally run the ISMS. No specific information about the process is contained in ISO/IEC [20] and [49].

The resource management process needs to be carried out on a regular basis, because it is integrated in the ISMS and continuously supports the ISMS processes. This process is also supporting the controls by means of the identification, allocation and monitoring of required resources. So, this is not a one-time task.

The resource management process could also 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. But 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. Consequently, the risk owners are the direct customers of this process. Taking this into account, 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. This process is also part of the service management system. While planning the integration of an ISMS with a service management system, this enables synergy effects by planning an integrated instead of two separate processes.

4.6 Process to assure necessary awareness

The process to assure necessary awareness consists on the development and implementation of an information security awareness, training and education program. Objectives of the process are to ensure that all personnel receive 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 the implications of not conforming with ISMS requirements.

Of course this process needs to be carried out regularly, because requirements, risks and controls as well as the employees/personnel are continuously changing. This process also transforms inputs like awareness requirements, policies and security objectives into awareness plans, materials and, finally, an adequate awareness level of all employees.

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.

Ensuring that all employees have the necessary competence (as part of this process as it is documented in ISO/IEC [20]), rather seems to be the responsibility of the human resources department. Given that the process to assure necessary awareness focusses only at the awareness of the employees.

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.

4.7 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 [51, p. 22]. In the risk communication process inputs like information about risks and information needs of stakeholders are transformed into risk communication plans. Information needs of the stakeholders are satisfied.

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

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

4.8 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. While processing records and other operational documentation, the process itself is operationally too.

In practice, document management is often not the core competency of ISMS staff. Nevertheless, to manage an appropriate documentation and records is a responsibility of the information security officer, because this documentation enables him or her to provide evidence of an appropriate ISMS.

Providing access to information necessary to assess 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 or she 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, enable the employees to have access to relevant ISMS documents which will lead to a higher security level.

This process is also part of the service management system. Again, synergy effects appear when the integration of ISMS and service management is made possible.

4.9 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. As it is necessary to continually keep the identified requirements up-to-date, this process is performed regularly. The process transforms inputs like stakeholder expectations and other constraints into documented and assigned requirements. Information security requirements identification is performed while operating the ISMS. Identifying all relevant requirements for information security is not only the responsibility of the information security officer – it is also one of the core competencies of the ISMS. Identified and assigned requirements are 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.

4.10 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 in a regular basis, 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. Changes occur at all levels – strategic, tactic and operational. 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. Because of the focus of this process, it must also be a core competency of the ISMS.

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 [52], the change management clearly provide a direct value for the stakeholders.

This process is also part of the information security management processes of the service management system [35, pp. 18–19]. One more time, synergy effects appear when the integration of ISMS and service management is made possible.

4.11 Process to control outsourced services

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

This is mainly achieved by analyzing drafts or final contracts in order to check if security requirements are met and if the development of requests for changes regarding requirements stipulated in contracts are performed. Finally, it is intended to check the conformance of the planning and execution of service provider audits regarding compliance with information security requirements. The process to control outsourced services needs to be repeated on a regular basis.

Within the process to control outsourced services, inputs like requirements are transformed into specific phrases in contracts or request for changes.

The process to control outsourced services is focused on ensuring information security and 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 and clearly within the core competency of the ISMS.

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

This process is also part of the service management system [35, pp. 18–19]. Again, synergy effects appear when the integration of ISMS and service management is made possible.

4.12 Performance evaluation process

The performance of an ISMS should be monitored regularly [49, p. 63]. The performance of controls like continuity controls should also be verified regularly [21, p. 73]. Both, the performance evaluation of ISMS processes as well as the performance evaluation of controls are realized within the performance evaluation process.

This process is also part of the service management system [35, p. 16], where it is used to monitor trends and performance against service targets. One more time, synergy effects appear when the integration of ISMS and service management is made possible.

Inputs like control lists and control objectives are transformed into monitoring/measurement activities as well as records of those activities and, finally, in management reports.

According to ISO/IEC 27003:2010 [49, p. 63], the measurement process should be integrated into the ISMS cycle. The seamlessly integration of this process in the ISMS cycle requires that this process is a core competency of the ISMS.

Results of this process like management reports are a direct value for the top management (stakeholders) as they support decision making of the top management [49, p. 63] regarding ISMS-related decisions and improvement of the ISMS [53, p. vii]. Additionally, performance evaluation is one of the critical success factors of the ISMS [54, p. 11].

4.13 Internal audit process

The results of this process are inputs for the regularly evaluation of the ISMS this process must performed in a regular basis [49, p. 41,55].

Inputs like control lists, control objectives and incident reports are transformed into audit plans, audit reports and, finally, in management reports. Internal audits regarding information security controls are an integral part of the check phase in the PDCA 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.

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 division is necessary because independence if 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. The seamless integration of this process in the ISMS cycle requires that this process is a core competency of the ISMS.

Results of this process like audit and management reports are a direct value for the top management (stakeholders) as they support decision making of the top management [49, p. 63] regarding ISMS-related decisions and improvement of the ISMS [53, p. vii]

This process is also part of the service management system [35, pp. 18–19]. Again, synergy effects appear when the integration of ISMS and service management is made possible.

4.14 Information security incident management process

Information security incidents should be detected and responded to in a timely manner [49, p. 63]. While it is not clear when and how often information security incidents occur, information about potential information security incidents is gathered regularly [55] and a continual proactive identification of information security incidents is conducted [56].

Potential information security incidents and gathered, information related to them is transformed into incident reports and changes are the basis for updating risk evaluations and training/awareness controls.

Information security incident management process (active prevention and detection of information security incidents) is a success factor of an ISMS [54, p. 7,11] and part of an operational ISMS [49, p. 31].

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.

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 [52]. Also, the top management has a direct benefit from the process resulting from the reduction of information security risks [54, p. 11].

This process is also part of the service management system [35, pp. 18–19]. One more time, synergy effects appear when the integration of ISMS and service management is made possible.

4.15 Information security improvement process

Continuous improvement of the ISMS and the information security controls are stipulated by ISO 27001 [20, 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.

Inputs like suggestions for improvement and nonconformities are transformed into request for changes to realize the improvement or to eliminate root causes of non-conformities.

The information security officer is owner of this process, as he or she is responsible for an effective and efficient ISMS. This process is carried out while operating the ISMS.

Results of this process like request for changes to improve the ISMS represent direct value for the top management (stakeholders) as they ensure that the ISMS is operated effectively and efficiently.

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

4.16 Information security customer relationship management

On the basis of [35, pp. 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;
- Establishment a method for measuring and demonstrating the value of information security and the efficient resource usage [40, 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;
- Establishment 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.

According to the COBIT process EDM02 [40, 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.

The information security customer relationship management process transforms inputs from the customers – like requirements and complaints – into changes in the ISMS or information security controls. This process needs 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.

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. Of course the business relationship management process is value generating as it ensures an appropriate customer satisfaction.

4.17 Configuration management process

The configuration management process ensures that every configuration item (CI) including their relationships to other CIs and service components is uniquely recorded in the configuration management database [35, pp. 22–23] which is used as input for most operational ISMS and SMS processes. Changes to CIs are also 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. 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. As this process is part of the service management system and it is not mentioned in the ISMS, the accountability lies within manager of the service management system.

5. Evaluation

To verify or dismiss the identified ISMS core processes or add missing ISMS core processes, the authors of this article conducted a study [48]. In this study, 90 experts were asked to name ISMS core processes in form of a questionnaire. 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; 8 working for private companies).

The set of possible ISMS core processes was given as shown in Table 2. Results of the study to identify ISMS core processes.

Table 2. Results of the study to identify ISMS core processes

Named process
ISMS planning process
Information security risk assessment process
Information security risk treatment process
Resource management process
Process to assure necessary awareness and competence
Communication process
Documentation control process
Requirements management process
Information security change management process
Process to control outsourced processes
Performance evaluation process
Internal audit process
Information security improvement process
Information security governance process
Information security incident management process
Service level management process
Service reporting process
Service continuity and availability management process
Budgeting and accounting for services process
Capacity management process
Business relationship management process
Supplier management process
Incident and service request management process
Problem management process
Configuration management process
Change management process
Release and deployment management process
Information security customer relationship management process

The detailed results of the study are described in Haufe et al. [48] and mainly confirmed the set of ISMS core processes proposed in this work.

The ISMS core process framework have been implemented and are operational in a medium-sized government organization as a pilot project. The first results of the pilot application are:

- 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 holistic ISMS process framework results in focusing on a process perspective rather than a measure perspective. 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. A holistic ISMS process framework as a starting point also prevents the implementing organization from researching the standards regarding ISMS processes, as they are already provided;
- Beside the modification of the ISMS processes, processes differ in the implemented maturity level. Especially the process to control outsourced services and the information security incident management process need to be implemented at a high maturity level in the piloting organization due to a significant dependability on the provided services;

- Some processes are not necessary at maturity levels of “defined” or lower. Examples are internal audit process, performance evaluation process, information security improvement processes;
- The process "Documents and records control process" should be divided in "Security policy management process" (ISMS core process) from Veiga and Eloff [50] and "Records control process" (Support process).

To sum up the initial evaluation results, implementing the proposed ISMS process framework has the following advantages compared to the traditional measurement or control-objective-driven approach:

- Efficiency – the implementing organization does not need to research possible ISMS processes in the ISO standards, as they are provided with the framework;
- Operational focus – by implementing the ISMS process framework the focus is shifted from control objectives to a process oriented view, which better enables and supports an operation of an ISMS.

6. Conclusions and future work

The pilot implementation of the proposed ISMS process framework proved that a process-oriented view of the ISMS can help focusing on the operation of an ISMS and improve the efficiency while planning such processes. By this, as a main finding, the systemic character of the ISMS consisting of processes and the perception of relevant roles of the ISMS is strengthened.

The pilot implementation also showed that some improvements of the framework need to be done and that an unadjusted implementation of the framework will not be sufficient. Given that the future work will consist of three steps:

Step 1: Improvement of the framework

In the future, the first and further results of the evaluation of the proposed ISMS process framework should be analyzed and used to improve the framework. Especially already available results of the pilot implementation will be used and the process "Documents and records control process" will be divided in "Security policy management process" (ISMS core process) from Veiga and Eloff [50] and "Records control process" (Support process). Those processes will be integrated in the framework.

Step 2: Development of a method to adjust and make costs for operating the ISMS core processes transparent.

Transparency of information security costs could be further improved by tailoring the maturity level of ISMS processes to the requirements of the organization. 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 [25, p. 8]. 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.

Step 3: Derive a basic process framework for lower maturity levels

The pilot implementation of the proposed ISMS process framework showed that, especially in the case of organizations were the overall maturity level of the ISMS is not higher than “defined”, the proposed process framework is too complicated and too big. For those organizations, a modified basic ISMS core process framework should be derived. This framework could also be a milestone for organizations which want to establish a higher maturity by an iterative approach.

References

[1] T. R. Peltier, *Information security fundamentals*. CRC Press, 2013.

[2] A. Calder, *Information Security Based on ISO 27001/ISO 27002: A Management Guide*. Van Haren Publishing, 2009.

[3] A. Alvaro, "Sicherheit in der Informationsgesellschaft," in *Freiheit: gefühlt–gedacht–gelebt*, Springer, 2009, pp. 214–227.

[4] M. Kittel, T. J. Koerting and D. Schött, *Kompendium für ITIL-Projekte*. readIT, 2006.

[5] German Federal Office for Information Security, *BSI-Standard 100-1*. Bonn, 2008.

[6] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 27000 series*. Geneva.

[7] M. Whitman and H. Mattord, *Management of information security*. Cengage Learning, 2013.

[8] B. Fakhri, N. Fahimah and J. Ibrahim, "Information Security Aligned To Enterprise Management," *Middle East Journal of Business*, vol. 10, no. 1, 2015.

[9] S. Dzombeta, V. Stantchev, R. Colomo-Palacios, K. Brandis and K. Haufe, "Governance of Cloud Computing Services for the Life Sciences," *IT Professional*, vol. 16, no. 4, pp. 30–37, Jul. 2014.

[10] L. Lema, J.-A. Calvo-Manzano, R. Colomo-Palacios and M. Arcilla, "ITIL in small to medium-sized enterprises software companies: towards an implementation sequence," *Journal of Software: Evolution and Process*, vol. 27, no. 8, pp. 528–538, Aug. 2015.

[11] T. Lucio-Nieto, R. Colomo-Palacios, P. Soto-Acosta, S. Popa and A. Amescua-Seco, "Implementing an IT service information management framework: The case of COTEMAR," *International Journal of Information Management*, vol. 32, no. 6, pp. 589–594, Dec. 2012.

[12] J. Eloff and M. Eloff, "Information security architecture," *Computer Fraud & Security*, vol. 2005, no. 11, pp. 10–16, 2005.

[13] R. Baskerville, P. Spagnoletti and J. Kim, "Incident-centered information security: Managing a strategic balance between prevention and response," *Information & Management*, vol. 51, no. 1, pp. 138–151, 2014.

[14] W. Pieters, C. W. Probst, S. Lukszo and L. Montoya, "Cost-effectiveness of Security Measures: A model-based Framework," *Approaches and Processes for Managing the Economics of Information Systems*, p. 139, 2014.

[15] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.

[16] L. A. Gordon and M. P. Loeb, "Budgeting process for information security expenditures," *Communications of the ACM*, vol. 49, no. 1, pp. 121–125, 2006.

[17] V. Sambamurthy, A. Bharadwaj and V. Grover, "Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms," *MIS quarterly*, pp. 237–263, 2003.

[18] A. Martins and J. Elofe, *Information security culture*. Springer, 2002.

[19] L. D. Bodin, L. A. Gordon and M. P. Loeb, "Evaluating information security investments using the analytic hierarchy process," *Communications of the ACM*, vol. 48, no. 2, pp. 78–83, 2005.

[20] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 27001:2013*. Geneva, 2013.

[21] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 27002:2013*. Geneva, 2013.

[22] German Federal Office for Information Security, *IT-Grundschutz Catalogues*, 13th ed. Bonn, 2013.

[23] U.S. Department of Commerce - National Institute of Standards and Technology, *NIST Special Publication 800 series*. Gaithersburg.

[24] M. Stoll, "An Information Security Model for Implementing the New ISO 27001," *Handbook of Research on Emerging Developments in Data Privacy*, p. 216, 2014.

[25] Information Systems Audit and Control Association, *IT-Governance and Process Maturity*. Rolling Meadows, 2008.

[26] W. Boehmer, "Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001," *SECURWARE*, vol. 8, pp. 224–231, 2008.

[27] J. Brenner, "ISO 27001: Risk management and compliance," *Risk Management Magazine*, vol. 54, no. 1, p. 24, 2007.

[28] Office of Government Commerce, *ITIL v3 Service Design*. London, 2007.

[29] Office of Government Commerce, *ITIL v3 Service Improvement*. London, 2007.

[30] Office of Government Commerce, *ITIL v3 Service Lifecycle*. London, 2007.

[31] Office of Government Commerce, *ITIL v3 Service Operation*. London, 2007.

[32] Office of Government Commerce, *ITIL v3 Service Strategy*. London, 2007.

[33] Office of Government Commerce, *ITIL v3 Service Transition*. London, 2007.

[34] V. H. Publishing, *IT service management: an introduction*. Van Haren Publishing, 2007.

[35] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 20000-1:2011*. Geneva, 2011.

[36] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 20000-2:2012*. Geneva, 2012.

[37] Information Systems Audit and Control Association, *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows.

[38] Information Systems Audit and Control Association, *COBIT 5 Enabling Processes*. Rolling Meadows.

[39] Information Systems Audit and Control Association, *COBIT 5 Process Assessment Model (PAM): Using COBIT 5*. Rolling Meadows.

[40] Information Systems Audit and Control Association, *COBIT 5 for Information Security*. Rolling Meadows.

[41] G. Ridley, J. Young and P. Carroll, "COBIT and its Utilization: A framework from the literature," in *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, 2004, p. 8.

[42] S. Sahibudin, M. Sharifi and M. Ayat, "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*, 2008, pp. 749–753.

[43] B. Von Solms, "Information Security governance: COBIT or ISO 17799 or both?," *Computers & Security*, vol. 24, no. 2, pp. 99–104, 2005.

[44] H. Susanto12, M. N. Almunawar and Y. C. Tuan, "Information security management system standards: A comparative study of the big five," *International Journal of Electrical Computer Sciences*, vol. 11, no. 5, pp. 23–29, 2011.

[45] C. Pardo, F. J. Pino, F. García, M. Piattini and M. T. Baldassarre, "A process for driving the harmonization of models," in *Proceedings of the 11th International Conference on Product Focused Software*, 2010, pp. 51–54.

[46] K. Haufe, R. Colomo-Palacios, S. Dzombeta, K. Brandis and V. Stantchev, "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, 2016.

[47] J. A. Calvo-Manzano, G. Cuevas and M. Muñoz, "Project Management Similarity Study: Experiment on Project Planning Practices Based on CMMI-Dev v1.2," in *EuroSPI 2008 - Proceedings*, Dublin, 2008, p. 11.

[48] K. Haufe, R. Colomo-Palacios, S. Dzombeta, K. Brandis and V. Stantchev, "ISMS core processes: A study," 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, 2016.

[49] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 27003:2010*. Geneva, 2010.

[50] A. D. Veiga and J. H. Eloff, "An information security governance framework," *Information Systems Management*, vol. 24, no. 4, pp. 361–372, 2007.

[51] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 27005:2011*. Geneva, 2011.

[52] D.-K. M. Nofer, O. Hinz, J. Muntermann and H. Rossnagel, "The Economic Impact of Privacy Violations and Security Breaches," *Business & Information Systems Engineering*, vol. 6, no. 6, pp. 339–348, 2014.

[53] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 27004:2010*. Geneva, 2010.

[54] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 27000:2014*. Geneva, 2014.

[55] J. D. Howard and T. A. Longstaff, "A common language for computer security incidents," *Sandia National Laboratories*, 1998.

[56] E. Humphreys, "Information security management standards: Compliance, governance and risk management," *information security technical report*, vol. 13, no. 4, pp. 247–255, 2008.

Biographical notes

Knut Haufe
Knut Haufe is a PhD candidate at the Universidad Carlos III de Madrid. He is also Lead Expert for information security management systems at PERSICON corporation, Germany and has more than ten years of experience as project manager for information security, audits and audit-preliminary consulting related to the German IT baseline security manual from the BSI (Federal Office of Information Security) and ISO 27001. Knut Haufe holds a Master in Commercial Law (LL.M. Com.) from the University of Kaiserslautern, Germany and a Diplom in Wirtschaftsinformatik (business informatics) from the Technical University of Ilmenau, Germany. He is also a member of the Standards Committee on Information Technology and Applications (NIA) 043-01-27-01 of the DIN (German Institute for Standardization which represents German interests within ISO, the International Organization for Standardization) which works on information security management system standards.

www.shortbio.net/khaufe@persicon.com

Ricardo Colomo-Palacios
Full Professor at the Computer Science Department of the Østfold University College, Norway. Formerly he worked at Universidad Carlos III de Madrid, Spain. His research interests include applied research in Information Systems, IT project management and people in IT projects among others. He received his PhD in Computer Science from the Universidad Politécnica of Madrid (2005). He also holds a MBA from the Instituto de Empresa (2002). He has been working as Software Engineer, Project Manager and Software Engineering Consultant in several companies including Spanish IT leader INDRA. He is also an Editorial Board Member and Associate Editor for several international journals and conferences and Editor in Chief of International Journal of Human Capital and Information Technology Professionals. He has published more than two hundred works in journals, books and conferences.

www.shortbio.net/ricardo.colomo-palacios@hiof.no

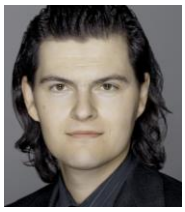
Srdan Dzombeta
Srdan Dzombeta is a business graduate and Master in Commercial Law (LL.M. Com.). He studied at the Technical University Berlin, the University of California in Los Angeles and Saarland University. Srdan Dzombeta is the partner with responsibility for governance and compliance and deals with implementing the propriety requirements for relevant processes and procedures when using information technology. Srdan Dzombeta gained experience in the use of national and international legal norms and recognized standards particularly while working for several years with a leading international accounting firm. For example, he was manager for planning and executing various consulting and auditing projects in the fields of telecommunication, finance, post and transport/logistics together with technology/IT outsourcing.

www.shortbio.net/sdzombeta@persicon.com

Knud Brandis

Knud Brandis studied law at the University of Potsdam and acquired his Master of Business Administration (MBA) in Financial Management from the University of Wales (UK) in 2005. As a Partner at PERSION, he is responsible for the information security and risk management department. He is primarily engaged with the management- and control aspects. Among other positions Knud Brandis held, he gained his experience in the implementation of national and international standards through his long engagement as a senior audit manager for a leading international accounting company in New York. He is co-author of the IT-baseline security catalogue (previously IT-security handbook) of the German Federal Office for Information Security. Knud Brandis is also lecturer for the Master course "information security management" at Brandenburg college, for "IT-Service management according to ITIL" at the dual education college in Villingen-Schwenningen as well as for "Consulting" at the Berlin School of Economics and Law.

www.shortbio.net/kbrandis@persicon.com



Vladimir Stantchev

Vladimir Stantchev is the executive director of the Institute of Information Systems at SRH University Berlin where he is a research professor. He is also a professor at the University of Granada, Spain and an affiliated senior researcher with the Networking Group at the International Computer Science Institute (ICSI) in Berkeley, California, USA. Vladimir Stantchev studied law at Sofia University (Sofia, Bulgaria) and also earned his master's degree in computer science from the Humboldt-University in Berlin, Germany. He received his PhD (Dr. rer. nat.) in the area of system architectures from the EECS department of the Berlin Institute of Technology (TU Berlin). His major research interests are in the areas of IT-Governance, Cloud Computing architectures, IT strategy, as well as methods for service and software engineering.

www.shortbio.net/vladimir.stantchev@srh-hochschule-berlin.de