Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 100 (2016) 755 – 761

Procedia Computer Science

Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016, October 5-7, 2016

Security Management Standards: A Mapping

Knut Haufe[a], Ricardo Colomo-Palacios[b*]
Srdan Dzombeta[a], Knud Brandis[a],Vladimir Stantchev[c]

[a]*Persicon Corporation, Friedrichstraße 100, 10117 Berlin, Germany, {khaufe,sdzombeta,kbrandis}@persicon.com*
[b]*Østfold University College, Norway, ricardo.colomo-palacios@hiof.no*
[c]*SRH Hochschule Berlin, Berlin, Germany, vladimir.stantchev@srh-hochschule-berlin.de*

Abstract

Adjustment and cost-effectiveness are key elements of a successful Information Security Management System (ISMS). ISMS-Processes, as basic elements of every ISMS, need to be aligned to the organization and its mission. As of today, a specific ISMS process framework does not exist. ISMS processes are not in focus of current research. This article aims to fill this research gap by presenting results of a process mapping study regarding ISMS processes in the most important and widely accepted international standards for Information Security Management. Authors propose a set of ISMS processes within an ISMS process framework which should be implemented at an individually appropriate maturity level.

Peer-review under responsibility of the organizing committee of CENTERIS 2016

Keywords: Information Security, ISMS, Mapping, Processes, IT Governance

1. Introduction

Information security is an integral element of fiduciary duty that is considered a subset of IT governance [1]. The purpose of information security is to protect an organization's valuable resources, such as information [2]. In relevant standards and frameworks as well as in the literature the continuously increasing dependency of nearly all organizations on appropriate secure information processing was reported, e.g. [3], [4]. Standards for the management of information security and collections of best practice measures were developed and established[5],

* Corresponding author. Tel.: +47 6921 5000; fax: +47 69 21 50 03.
E-mail address: ricardo.colomo-palacios@hiof.no

Peer-review under responsibility of the organizing committee of CENTERIS 2016
doi:10.1016/j.procs.2016.09.221

[6]. According to [7] the most important and most widely accepted international initiatives for the development and operation of an ISMS are ISO 270xx, ITIL [8] and COBIT [9], also relevant in aspects like information and security management [10], [11], as well as cloud governance [12]. 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. Integration of these activities into a process framework for information security that makes explicit the interrelationships will enable a cost-effective security[13], but their activities tend to be viewed as silos. Over the last few years, cost benefit discussions have influenced information security practice[14]. The value of information must justify protection costs. Adjustment and cost-effectiveness are key elements of a successful ISMS [2]. Knowledge of the mission is needed to align the ISMS processes to the organization and their mission [15]. Taking into account the importance of business alignment and cost-effectiveness for the successful operation of an ISMS, research contributions should address both problems by enabling a clear identification of necessary and appropriate ISMS processes as core elements of every ISMS.

The problem is, that actually such a process framework for security management does not exist. This is still a problem because information security management is a complex issue [16] and current research focuses on economics and cost benefit analysis of information security investment regarding single measures protecting information. The ISMS and the ISMS processes themselves are in focus of current research [17], [18].

This article aims to fill this research gap by presenting results of a process mapping study regarding ISMS processes. The mapping study will answer the research question “Of which elements does the agreed ISMS core process framework consists?”. This research question is decomposed into the following sub-questions:

1. Which processes are described in the established security management standards and to what extend they are related?
2. Which of the identified processes are ISMS processes?

General mappings and integrations between/of COBIT, ITIL and ISO/IEC27000 series are already available [19], [20]. But those mappings are either general, control focused or requirements focused. To the best of authors’ knowledge, there is not a mapping focused on processes mentioned in those standards available. The results of a mapping focused on processes enabled the authors to develop and contribute an agreed-upon ISMS process framework to the current body of knowledge. The outcome is a detailed set of ISMS processes including process descriptions (process profiles) and process flow charts – which are included only at a high level because it would disrupt the scale of this paper. These ISMS processes within an ISMS process framework should be implemented at an individually appropriate maturity level. This helps the practitioners to manage information security more efficiently and effectively which is finally the overall objective of the proposed framework.

The rest of the article is structured as follows: in section 2 authors describe the methods for the analysis of security management standards, while section 3 presents the results of the analysis of security management standards. Finally, section 4 wraps up the paper and present future works.

2. Methods for the analysis of security management standards

To answer the first research question, the objective of the analysis of security management standards can be summarized as follows:

- Analyze ISO 27001 standard statements on processes
- for the purpose of comparing it
- with respect to the degree of coverage and relationship with specific processes in ITIL and COBIT in favouring 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

To reach this objective, multiple process reference models need to be harmonized. Baldassarre [21] 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 [22]. According to Baldassarre [21] "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.

A theoretical comparison process is used as the harmonization process, because mapping is one of the most widely used strategies for the harmonization of models [21]. The purpose of this process is to perform a step-by-step comparison and a mapping of different models, aiming to guarantee the reliability and robustness of obtained results. For the theoretical comparison the ISO 27001 standard was considered as a starting model, as it is considered the most important standard for information security management [9].

The outcome of the theoretical comparison process is a table (Result of Comparison) that maps the models and points out the relationships between them regarding the mentioned ISMS processes.

An adaptation on the Models and Standards Similarity Study method [22] was used for the analysis of the identified security management standards. The method adapted to the aims of this study is as follows:

1. Select the models and standards to be analyzed – this step is documented in section 1
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 is described in section **Error! Reference source not found.**.
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 – The obtained results are described in section 3.

The terms matching and mapping are differentiated as follows: Matching is the process of identifying two semantically related processes [23]. Processes are semantically related if they are represented (analogy) in two or more standards with the same or different terms. The interpretation rules to decide if there is an analogy are characterized as implicit rules for mapping knowledge about a base domain (ISO 27000 series) into a target domain [24]. Beside this, a comparison scale has been defined and used. The scale contains the following elements based on the scale presented by Baldassarre [21]:

- 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.

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 [24]. Matching and mapping are established methods in scientific knowledge comparison [25] and especially used to compare and merge different ontologies [23], [24]. In the step of matching, the comparison is performed through an iterative and incremental procedure. The process used (adapted from [21]), 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. The result of this task is documented in section 3.
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. The result of this task is documented in section 3. In the context of the matching the following questions were asked (based on[22]):
    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 section 3

3. Results of the analysis of security management standards

The analyzed standards do not provide an ISMS process framework including a detailed description of ISMS processes, input, outputs and interfaces of the processes. Table 1 - matrix of analyzed standards and contained ISMS processes contains a matrix of analyzed standards and the identified possible ISMS processes, which will answer the first research question: “What processes in the established security management standards are described and to what extend are they related?”

Table 1 - matrix of analyzed standards and contained ISMS processes

Process/standard	ISO 27000 series	ITIL	COBIT
ISMS planning process	X	– (N)	X (S)
Information security risk assessment process	X	X (S)	X (S)
Information security risk treatment process	X	– (N)	X (S)
Resource management process	X	X (P)	X (S)
Process to assure necessary awareness and competence	X	– (N)	X (S)
Communication process	X	– (N)	X (P)
Documentation control process	X	X (S)	X (P)
Requirements management process	X	– (W)	X (S)
Information security change management process	X	X (S)	X (S)
Process to control outsourced processes	X	X (S)	X (S)
Performance evaluation process	X	X (S)	X (S)
Internal audit process	X	X (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 (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)	X (W)	X (S)
Budgeting and accounting for services process	(X)	X (P)	X (S)
Capacity management process	(X)	X (W)	X (S)
Business relationship management process	–	X (N)	X (S)
Supplier management process	X	X (P)	X (S)
Incident and service request management process	(X)	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)

4. Conclusions and future work

As a prerequisite to answer the second research question criteria for the categorization of processes as ISMS core process were developed by analyzing relevant state of the art publications. The following basic criteria for ISMS core processes were identified and confirmed in a previous study from 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.

Applying the defined criteria for ISMS core processes to the results of the mapping a list of ISMS core processes was concluded. Table 2 - Identified ISMS core processes contains the result of matching the identified processes against the criteria for ISMS core processes. “X” indicates that the process fulfills the criteria fully and “(X)” indicates that the process fulfills the criteria to a certain degree.

Table 2 - Identified ISMS core processes

Process/criteria	Regula-rity	Trans-formation	Opera-tionally	Accoun-tability	Process/ criteria
Information security risk assessment process	X	X	X	X	X
Information security risk treatment process	X	X	X	X	X
Resource management process	X	X	X	X	(X)
Process to assure necessary awareness and competence	X	X	X	(X)	X
Communication process	X	X	X	X	X
Documentation and records control process	X	X	X	X	X
Requirements management process	X	X	X	X	X
Information security change management process	X	X	X	X	X
Process to control outsourced processes	X	X	X	X	X
Performance evaluation process	X	X	X	X	X

Internal audit process	X	X	X	(X)	X
Information security incident management process	X	X	X	X	X
Information security improvement process	X	X	X	X	X
Information security customer relationship management process	X	X	X	X	X

The added value of this framework is a shift from the requirements or control oriented approach of the COBIT, ITIL and ISO/IEC27000 standards towards a more practitioner and operations oriented approach. By using this framework practitioners e.g. information security officers easily can overview for which processes they are responsible to manage. This framework helps information security professionals to focus on the operation of an ISMS and not to get lost in the increasingly unmanageable amount of information security controls and measures. Also using this process oriented approach enables the practitioners to include a maturity discussion regarding every ISMS process which finally will enable the information security officer to align the maturity of the ISMS processes – and with that the ISMS itself – to the requirements of the organization. This helps the practitioners to manage information security more efficiently and effectively which is finally the overall objective of the proposed framework. So typical uses of this framework are ideally while planning and implementing an ISMS or – if a first adoption of an ISMS is already in place – while operating an ISMS to focus on the operation.

To ensure efficiency and effectiveness the ISMS-processes should be subject to a standardization process in large organizations and organization with multiple or even multinational sites [26].

The analysis of the security management standards aims at meeting the research criteria of relevance, applicability and specificity [27]. Our work meets those criteria:

- Relevance – taking into account the increasing dependability of organizations from information processing an effective and efficient information security management is highly relevant to nearly all organizations
- Applicability – the proposed ISMS process framework is applicable to all organizations independent of their size, objectives, business model, location et cetera as the underlying international standards are
- Specificity – differentiating a set of 14 ISMS processes supported by generalized process descriptions, process profiles and process flow-charts are much more specific than in actual research in this field or in the included information in the underlying standards.

For including maturity discussions further research is necessary as to the best of the authors knowledge there is no agreed method present how to determine the necessary maturity level of ISMS-processes or even processes in general. 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 [28]. Current research regarding maturity levels only focus on the determination of the actually reached maturity level. Research regarding determining the necessary maturity level of processes will be part of a next research phase of the authors. Other activities will address the integration of the approach as characteristics of cloud services offered on cloud marketplaces [29] and in the application domain of healthcare [30].

References

[1] A. Calder, *Information Security Based on ISO 27001/ISO 27002: A Management Guide*. Van Haren Publishing, 2009.
[2] T. R. Peltier, *Information security fundamentals*. CRC Press, 2013.
[3] H. Cavusoglu, H. Cavusoglu, J.-Y. Son, and I. Benbasat, “Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources,” *Inf. Manage.*, vol. 52, no. 4, pp. 385–400, Jun. 2015.
[4] S. Dzombeta, V. Stantchev, R. Colomo-Palacios, K. Brandis, and K. Haufe, “Governance of Cloud Computing Services for the Life Sciences,” *IT Prof.*, vol. 16, no. 4, pp. 30–37, Jul. 2014.
[5] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 27001:2013*. Geneva, 2013.
[6] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 27002:2013*. Geneva, 2013.
[7] H. Susanto12, M. N. Almunawar, and Y. C. Tuan, “Information security management system standards: A comparative study of the big five,” *Int. J. Electr. Comput. Sci. IJECSIJENS*, vol. 11, no. 5, pp. 23–29, 2011.

[8] Office of Government Commerce, *ITIL v3 Service Design*. London, 2007.
[9] M. Stoll, “An Information Security Model for Implementing the New ISO 27001,” *Handb. Res. Emerg. Dev. Data Priv.*, p. 216, 2014.
[10] 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,” *Int. J. Inf. Manag.*, vol. 32, no. 6, pp. 589–594, Dec. 2012.
[11] 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,” *J. Softw. Evol. Process*, vol. 27, no. 8, pp. 528–538, Aug. 2015.
[12] V. Stantchev and L. Stantcheva, “Extending Traditional IT-Governance Knowledge Towards SOA and Cloud Governance,” *Int. J. Knowl. Soc. Res. IJKSR*, vol. 3, no. 2, pp. 30–43, 2012.
[13] Information Systems Audit and Control Association, *An Introduction to the Business Model for Information Security*. Rolling Meadows, 2009.
[14] M. Whitman and H. Mattord, *Management of information security*. Cengage Learning, 2013.
[15] B. Fakhri, N. Fahimah, and J. Ibrahim, others, “Information Security Aligned To Enterprise Management.,” *Middle East J. Bus.*, vol. 10, no. 1, 2015.
[16] R. Baskerville, P. Spagnoletti, and J. Kim, “Incident-centered information security: Managing a strategic balance between prevention and response,” *Inf. Manage.*, vol. 51, no. 1, pp. 138–151, 2014.
[17] L. A. Gordon and M. P. Loeb, “The economics of information security investment,” *ACM Trans. Inf. Syst. Secur. TISSEC*, vol. 5, no. 4, pp. 438–457, 2002.
[18] L. A. Gordon and M. P. Loeb, “Budgeting process for information security expenditures,” *Commun. ACM*, vol. 49, no. 1, pp. 121–125, 2006.
[19] B. Von Solms, “Information Security governance: COBIT or ISO 17799 or both?,” *Comput. Secur.*, vol. 24, no. 2, pp. 99–104, 2005.
[20] 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.
[21] 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.
[22] J. A. Calvo-Manzano, G. Cueva, 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.
[23] D. Gentner, “Structure-mapping: A theoretical framework for analogy,” *Cogn. Sci.*, vol. 7, no. 2, pp. 155–170, 1983.
[24] W. Guo and S. B. Kraines, “Explicit scientific knowledge comparison based on semantic description matching,” *Proc. Am. Soc. Inf. Sci. Technol.*, vol. 45, no. 1, pp. 1–18, 2008.
[25] International Organization for Standardisation and International Electrotechnical Commission, *ISO/IEC 27003:2010*. Geneva, 2010.
[26] C. Loebbecke and B. Thomas, “Developing and enforcing internal information systems standards: InduMaker’s Standards Management Process,” *Dev. Enforc. Intern. Inf. Syst. Stand. InduMaker’s*, vol. 4, no. 1, pp. 5–24, 2016.
[27] J. L. Cheng and W. McKinley, “Toward an integration of organization research and practice: A contingency study of bureaucratic control and performance in scientific settings,” *Adm. Sci. Q.*, pp. 85–100, 1983.
[28] Information Systems Audit and Control Association, *IT-Governance and Process Maturity*. Rolling Meadows, 2008.
[29] V. Stantchev and G. Tamm, “Reducing Information Asymmetry in Cloud Marketplaces,” *Int. J. Hum. Cap. Inf. Technol. Prof. IJHCITP*, vol. 3, no. 4, pp. 1–10, 2012.
[30] V. Stantchev, R. Colomo-Palacios, and M. Niedermayer, “Cloud Computing Based Systems for Healthcare,” *Sci. World J.*, vol. 2014, 2014.