

UNDERSTANDING THE MANAGEMENT OF INFORMATION SECURITY CONTROLS IN PRACTICE

Daniel Bachlechner¹, Ronald Maier¹, Frank Innerhofer-Oberperfler² and Lukas Demetz¹

¹Innsbruck University School of Management, Information Systems

²Institute of Computer Science, Quality Engineering

University of Innsbruck, Austria

{firstname.lastname}@uibk.ac.at

Abstract

The ever greater reliance on complex information technology environments together with dynamically changing threat scenarios and increasing compliance requirements make an efficient and effective management of information security controls a key concern for most organizations. Good practice collections such as COBIT and ITIL as well as related standards such as the ones belonging to the ISO/IEC 27000 family provide useful starting points for control management. However, neither good practice collections and standards nor scholarly literature explain how the management of controls actually is performed in organizations or how the current state-of-practice can be improved. A series of interviews with information security professionals from European organizations was conducted in order to better understand how a coherent and comprehensive suite of controls is built and maintained in practice and to help organizations refine related work practices. The interviews focused on the activities of control management as well as on the roles and responsibilities of the individuals and groups involved in those activities. The results of a qualitative content analysis of the gathered data allowed an aggregate description of control management on the basis of a generic control management cycle ranging from the creation of a control design to its implementation and review.

Keywords

Information security, security controls, control management, empirical study, qualitative content analysis, work practices, roles, responsibilities

INTRODUCTION

The US National Institute of Standards and Technology (NIST) defines information security controls as controls applied to information systems to protect the confidentiality, integrity and availability of systems and the information they process, store and exchange (NIST, 2008). It is widely agreed that information security is not per se a technical problem (Dhillon & Backhouse, 2000). Accordingly, the NIST (2008) classifies security controls into three categories. As opposed to technical controls such as user authentication and firewalls which are primarily executed by the information systems, operational controls such as incident response processes are not only implemented but also executed by people. Management controls focus on the management of risks and information security. Most organizations recognize the importance of information security and have a suite of controls in place (Brycezynski & Small, 2003). Information security, however, is not a state or condition of an information system or organization but an ongoing responsibility (Anderson & Rachamadugu, 2006).

Information security management is often associated with information security management systems (ISMSs) that arose primarily out of the international standard ISO/IEC 27001. The widely used standard claims to “ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested partners” (ISO/IEC, 2005). However, being certified as compliant with ISO/IEC 27001 does not say much about the quality of the implemented ISMS (Böhmer, 2008). The compliance certificate provides assurance that a management system for information security is in place, but neither technical nor operational controls are audited in ISO/IEC 27001 certification audits.

Good practice collections such as COBIT and ITIL are also often mentioned in the context of information security management. Certain COBIT processes and ITIL activities are concerned with control management and COBIT also provides suggestions regarding the assignment of roles and responsibilities. Von Solms and von Solms (2004) point out that both good practice collections and standards stress the importance of clarity regarding the performance of activities and the distribution of roles and responsibilities. However, neither good practice collections and standards nor scholarly literature provide detailed information on how the management

of controls actually is performed in organizations or how it can be improved. Nevertheless, a considerable number of scholarly publications addressed aspects of the management of information security controls (e.g., Baker & Wallace, 2007; Barnard & von Solms, 2000; Hagen et al., 2008; Siegel et al. 2002) and the distribution of information security roles and responsibilities (e.g., Höne & Eloff, 2002; Tudor, 2001), respectively, in the past.

The main goals of this paper are to understand how a coherent and comprehensive suite of security controls is built and maintained in practice and to provide organizations with clues for the refinement of related work practices. We discuss not only the commonalities and differences in the performance of control management activities but also the roles and responsibilities of selected groups involved in those activities. In increasingly complex and fast changing organizations, it becomes ever more important for employees to understand their roles and responsibilities. Dhillon and Backhouse (2000) list knowledge about roles and responsibilities among the four key principles for securing information assets in organizations. Clarity with respect to roles and responsibilities is considered particularly important for dealing with events that call for ad-hoc responses, not catered for in organizational charts, hierarchies or policies (Dhillon & Backhouse, 2000). Although security standards as well as national laws and regulations restrict the creative leeway of organizations, the study this paper builds upon revealed that control management approaches are manifold.

METHODS

This paper builds upon perceptions of information security professionals from large and medium-sized organizations in Europe collected within the scope of a series of twelve oral interviews conducted in the period from June 2009 to February 2010. The interviews took between 49 and 97 minutes, were tape recorded and focused on the activities of control management as well as on the roles and responsibilities of the ones involved in those activities. We made sure that the interviewees as well as the organizations they work for met several criteria.

Interviewees had to be information security professionals occupied with information security management activities for a considerable share of their working time or certified information security managers. They were expected to have had the responsibility for information security in organizations with rather complex information technology (IT) environments and they were required to have had at least three years of work experience in the field of information security. Regarding the organizations considered for our research, we made sure that the main sectors of economic activity were represented in the sample, that organizations of varying sizes had been included and that we had a well-balanced set of organizations with and without information security certification. Using a purposive sample allowed selecting interviewees who were able and willing to provide us with access to cases manifesting the phenomena under investigation intensely (Patton, 1990).

The collected data was analysed by means of a qualitative content analysis. Content analyses are systematic, rule-guided techniques to analyse the contents of textual data such as transcripts of interviews. There are several types of content analyses including quantitative and qualitative ones but all share the central idea of systematically categorizing data in order to make sense of them (Miles & Huberman, 1994). The various types of content analyses differ, however, not only with respect to the generation of codes and their application to the data but also with respect to the interpretation of the results. We chose a qualitative content analysis approach in which the codes were largely derived from the data and applied to the data through close reading.

The coding system included three main code families addressing different aspects of information security management. The first family of codes was used to annotate the groups and individuals involved, the second for the main activities and the third for the artefacts used. The coding system grew and evolved during the analysis, but the code families remained stable. By means of coding, text passages relevant for further analysis were extracted from the transcripts and categorized. The smallest coding unit was a sentence, the largest a paragraph.

After extraction and categorizing, the annotated text passages were prepared for interpretation. The preparation included sorting passages in the text with respect to commonalities and summarizing the ones having similar meanings. References to the source paragraphs in the transcripts were kept throughout the analysis. The material was then interpreted having the research goals in mind. We first evaluated the commonalities of the control management approaches characterized by the interviewees and used inductive reasoning to develop a generic control management cycle. Afterwards, we investigated the text passages addressing groups and individuals

involved in control management and assigned them, whenever possible, to the activities covered by the control management cycle.

RESULTS

It was no surprise to observe that the approaches to information security management in general and control management in particular were similar in many respects. However, when looking at the descriptions in more detail, we were able to identify not only several interesting differences but also recurring patterns. In the following, we describe the activities of control management as well as the roles and responsibilities involved in them. The description is the result of our interpretation of the different approaches to information security control management as they were described by the interviewees.

All organizations of our sample follow the principle of reassessment specified by the OECD (2002). Thus, based on the information provided by the interviewed information security professionals, a generic control management cycle reflecting the activities of control management and their sequence could be modelled. With its three phases, our control management cycle resembles the quality control cycle specified by Shewhart (1939). The Shewhart cycle served as foundation for the development of the four-phase PDCA cycle (Deming, 1986) which became an essential part of standards such as the quality management standard ISO 9001 or the aforementioned standard ISO/IEC 27001.

The *act* phase of the PDCA cycle generally expects taking corrective and preventive action after conducting a review in the *check* phase. However, in control management practice, after a review, the creation of a new control design is required before corrective and preventive action can be taken within the scope of the implementation of the new control design. Thus, for our purpose, a three-phase cycle appears to be more suitable. Figure 3 illustrates the generic control management cycle ranging from the creation of the control design to its implementation and review.

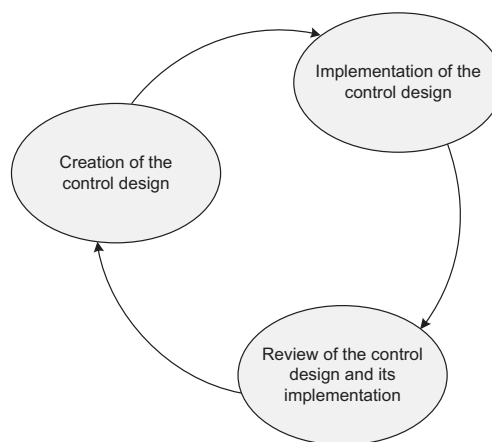


Figure 3 The generic control management cycle.

Most changes affecting the IT landscape and thus control requirements are made within the scope of projects. Minor changes, affecting not more than one system or organizational unit substantially, usually do not lead to the initiation of a project. Such changes are usually made autonomously by the system owner of the concerned system. Paying attention to security aspects is one of the key responsibilities of a project team or system owner when making a change to the IT landscape. One of the interviewees, for instance, stated that “as a matter of course the project manager is not only held liable if the planned project duration is exceeded but also if information security has not been taken into account adequately”. A typical project team consists of representatives of both the IT department and the functional departments affected by the change.

From a control management perspective, a project which was initiated for the purpose of an IT landscape change typically ends after the implementation of the control design has been completed. Around this point in time, the project team dissolves and the system owner takes over. The operation of a system in day-to-day business is usually also accompanied by members of the IT department and the functional departments but in

their roles as system administrators and system users. It is not unlikely that exactly the same individuals work with the system before, during and after the change which may or may not be conducted under the umbrella of a project. Being well aware of this situation, but for the sake of simplicity, we use the term *project team* at all times to refer to the members of the IT department and the functional departments involved in control management activities.

The security team is usually led by a C-level security officer. Most of the interviewees held this position at the organizations they work for. The team members are usually organized as a separate security department. We use the term *security team* to abstract from any organization-specific denominations. Under the term *management*, we subsume managers at all hierarchical levels from group managers up to the executive board.

Figure 4 shows that besides the project team, also the security team and the management are among the ones involved in control management. In some organizations, related activities are delegated to legal and HR units, respectively, and sometimes even customers or external consultants and auditors are involved. Internal auditors are considered members of the security team. Within the scope of this work, we focus on the project team, the security team and the management exclusively.

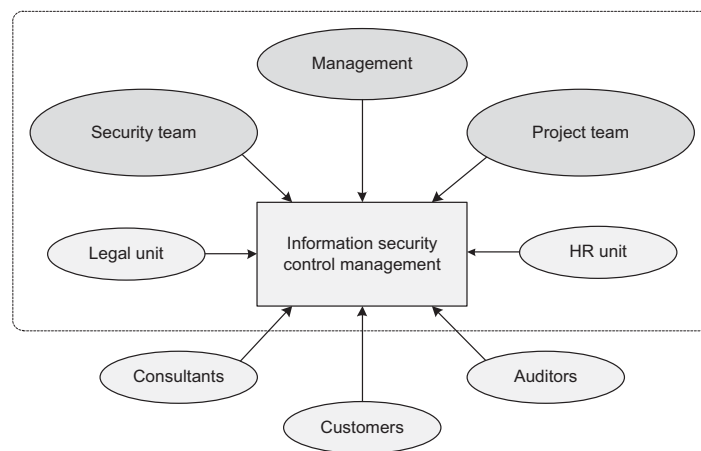


Figure 4 Groups and individuals involved in control management.

Below, the activities constituting the generic control management cycle are described in detail as they were portrayed by the interviewed information security professionals.

Creation of the control design

The creation of the control design is considered a three-part activity comprising the collection of control alternatives, the selection of the control alternatives to be implemented and the prioritization of the implementations.

Collection of control alternatives

Most interviewees reported that at the organizations they work for the project team is in charge of collecting control alternatives suitable to address identified needs for controls. One of the interviewees, for instance, explained that the members of the project team “work with the systems every day and usually have a fairly clear idea of what could be done”. According to him, it is often rather a matter of scarce funds, lack of time or missing decisiveness that certain controls were not already implemented earlier.

Selection of a subset of the control alternatives to be implemented

As long as the budget is not affected, the selection of the control alternatives to be implemented is also within the area of responsibilities of the project team. One of the interviewees, for instance, highlighted that “as long as there are no implications on the budget, the project team is absolutely free to select the control alternatives to be implemented”. Another interviewee stressed that the security team and the management also get involved if more than one organizational unit is affected.

Prioritization of the selected controls' implementations

It was reported that the responsibility for the prioritization of the implementations is often delegated to the security team and the project team, respectively. One interviewee reported, for instance, that at the organization he works for, “the security team makes its preferences plain but then the ones from the project team who actually implement the controls make the final decision“.

Implementation of the control design

The implementation of controls and the accreditation of information systems and services are sub-activities of the implementation of the control design.

Implementation of controls

With respect to the distribution of roles and responsibilities, there is a difference between the implementation of technical controls and the implementation of operational and management controls. Technical controls are usually implemented by the project team only. One interviewee, for instance, pointed out that “it is not the security team that implements the controls, the project teams are responsible for that but the security team monitors the implementation”. Most of the interviewees agreed that besides the project team also the security team and the management are involved in the implementation of operational and management controls. One interviewee reported, for instance, that “the security team, the respective project team and the management were involved in the creation and communication of a usage policy for handhelds”.

Accreditation of information systems

Activities related to the accreditation of new systems and the re-accreditation of systems after significant changes are led by the project team in most organizations of our sample. Accreditations are not only common for internal systems but also for services hosted externally. One of the interviewees, for instance, pointed out that while penetration tests are performed for internally operated systems, audit reports or certification confirmations are requested for services hosted externally. The security team is often involved in the accreditation of externally hosted services.

Review of the control design and its implementation

Besides the inspection of controls also the management of security incidents and efforts on staying up-to-date with respect to security-related topics are sub-activities of the review of the control design and its implementation.

Inspection of controls

Internal and external audits were reported as being the most common means to inspect existing controls and to identify needs for new controls. The inspection of controls is usually in the area of responsibility of the security team. One of the interviewees, for instance, pointed out that “the security team checks the implementation of all categories of security controls and calls attention to incomplete implementations”. Another interviewee highlighted that “the security team is in charge of achieving and maintaining an adequate level of security” and that after incidents, the work of the security team is often critically examined. Commissioning external audits is particularly common if organizations lack internal auditing expertise or if the credibility of internal audits would be low. One interviewee stated that “in order to assure the credibility of audits whose results may be relevant to customers, external audits are commissioned”.

Management of security incidents

The management of incidents also often leads to the identification of new needs for controls. Some of the interviewees stressed that there are different types of incidents which are addressed in different ways. One interviewee, for instance, explained that it is often challenging to distinguish between incidents which make an immediate action necessary and others which do not. According to the interviewee, “a virus on a personal computer or a server crash is usually not among the ones requiring immediate action”. Nevertheless, “every employee is encouraged to apply common sense and to report issues that may lead to security problems”. Incident management is usually coordinated by the security team. Members of project teams, however, are usually among the ones who recognize and react on incidents first.

Staying up-to-date with respect to security-related topics

The security team is usually the one mainly responsible for staying up-to-date with respect to security-related topics. One of the interviewees reported that the organization he works for exchanges security-related information with organizations active in the security industry but also with organizations in the same industry. In this context, the interviewee stated that “the good thing about information security is that all have the same enemies and that there is only little competition”. The security team usually forwards relevant information to members of the project teams in charge.

DISCUSSION

A more detailed version of the generic control management cycle incorporating the sub-activities discussed in the previous section is shown in Figure 5.

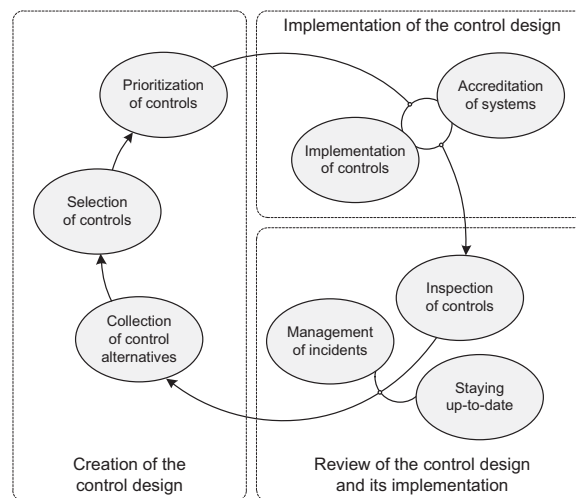


Figure 5 The generic control management cycle in detail.

Based on the information provided by the interviewees, we investigated not only the activities of control management in general but also the roles and responsibilities of the ones involved.

Figure 6 outlines the roles and responsibilities of the project team, the security team and the management. The project team is symbolized by a square with the letter *P*, the security team by a pentagon with the letter *S* and the management by a triangle with the letter *M* in its centre.

Summarizing the common thread between the different approaches to information security control management found at the organizations of our sample allowed the creation of a generic control management cycle which may not only be useful to better understand how a coherent and comprehensive suite of security controls can be built and maintained in practice but also to investigate to what extent good practice collections such as COBIT and ITIL or standards such as the ones belonging to the ISO/IEC 27000 family influence organizations in shaping their management of controls.

Furthermore, the detailed descriptions of the activities of control management as well as the characterization of the roles and responsibilities of the ones involved may serve as a point of reference for both researchers investigating the distribution or information security roles and responsibilities in practice and organizations attempting to make the management of their controls more efficient and effective. Last but not least, having a good understanding of the actual distribution of roles and responsibilities related to control management is considered an essential requirement for the improvement of the communication and coordination among organisational and external units on a macro level as well as among individuals on a micro level, no matter if the improvement is achieved through the use of IT – as it is attempted within the scope of the COSEMA project partially funding the research associated with this paper – or through any other means.

Below, an effort is made to provide high-level profiles of the project team, the security team and the management in the context of information security control management. The emphasis is not only on

commonalities among the tasks usually assigned to a specific group, but also on possible explanations for particular distributions of roles and responsibilities.

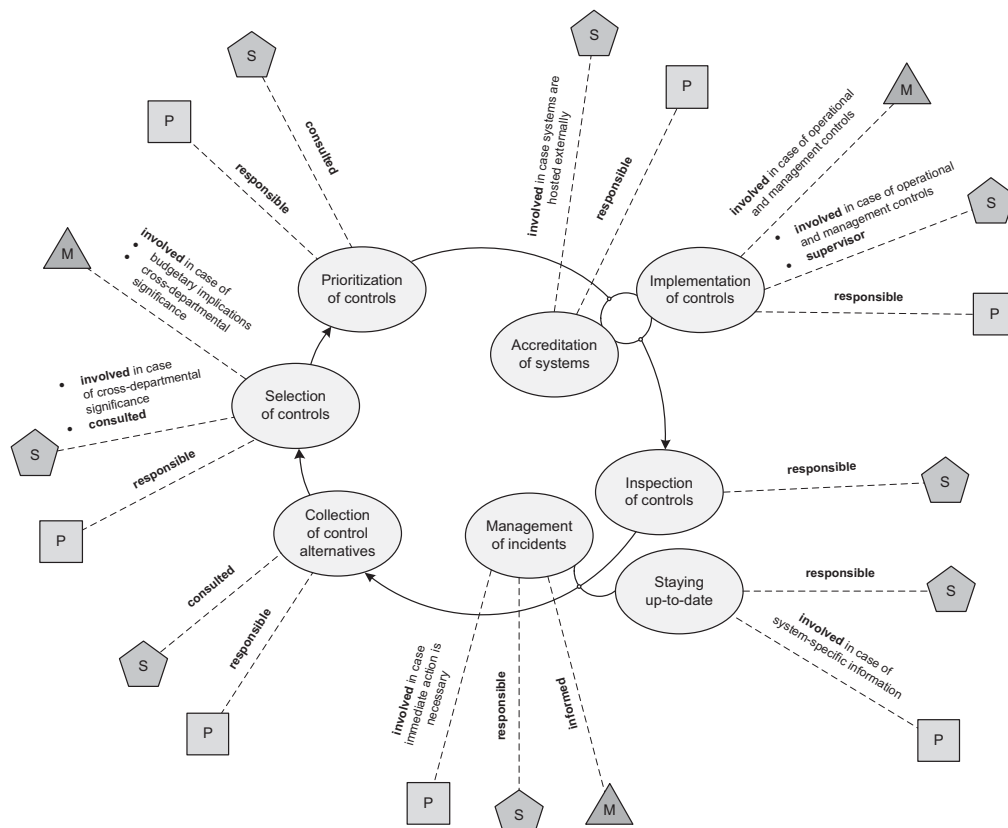


Figure 6 Selected groups involved in control management.

Project team

The project team is usually responsible for all sub-activities associated with the creation of the control design. The main reason for this is the expert knowledge of the members of the project team. The representatives of the functional departments usually have in-depth knowledge of the processes to be supported, whereas the representatives of the IT department are usually very confident and experienced regarding the technologies used. For the same reason, the project team is mainly responsible for the implementation of all categories of controls and the accreditation of information systems and services. The project team is usually not involved in the inspection of controls. However, the members of project teams operating systems in day-to-day business play a key role in the context of incident management. They are not only among the ones who usually recognize incidents first but also take immediate action if necessary. Finally, the members of project teams are involved in staying up-to-date with respect to system-specific information.

At its heart, the project team is, due to its expert knowledge, mainly responsible for creating the control design and implementing it. Under certain conditions, the security team and the management are also involved in these activities.

Security team

Regarding the creation of the control design, the security team usually has only advisory function. However, it gets involved into the selection process as a coordinator if more than one organizational unit is affected. The main reason for this is that the security team usually has a fairly complete picture of the control status at all units. Whenever the security team is not directly involved in the implementation of a control, it supervises it. Furthermore, the security team is involved in the accreditation of services hosted externally. The security team is usually mainly responsible for all sub-activities of the review of the control design and its implementation.

The security team's main responsibility is the inspection of controls. Furthermore, the security team is the central contact for reporting incidents and analyses related trends. Finally, the security team is in charge of staying up-to-date with respect to security-related topics. For this purpose, security teams are usually well networked.

In a nutshell, the security team is mainly responsible for the review of the control design and its implementation. Under certain conditions, the security team gets involved in the creation of the control design and its implementation, respectively, as an advisor, coordinator or supervisor.

Management

The management gets involved in the selection of the controls to be implemented in case the budget or a significant part of the organization is affected. The fact that most organizations do not have dedicated budgets for security makes the approval of the management necessary in case of budgetary implications. The main reason for the occasional involvement of the management in the implementation of operational and management controls lies in the particular importance of signalling management commitment for certain controls. With respect to the review of the control design and its implementation, the security team is merely receiver of aggregated incident reports compiled by the security team.

In summary, the management is only involved in control management activities under certain conditions, particularly, in case controls affect the budget or a significant part of the organization.

CONCLUSION

This paper described the performance of control management activities on the basis of a series of interviews with information security professionals. The presented generic control management cycle not only illustrates the interaction of the main activities but also how the project team, the security team and the management are usually involved in them. The control management cycle created by evaluating the commonalities of the approaches portrayed by the interviewees may be useful to better understand how a coherent and comprehensive suite of security controls can be built and maintained in practice.

From our perspective, the main contribution of this paper is the provision of a detailed overview of the main activities of control management and the involvement of selected groups. With its narrow focus and practical orientation, the overview goes beyond more general good practice collections and standards and may be a useful point of reference for organizations. It may help them to make the management of their controls more efficient and effective, and in consequence to become more resilient in times characterized by an ever greater reliance on complex IT environments together with dynamically changing threat scenarios and increasing compliance requirements.

Furthermore, it may also be a valuable complement to the scholarly discussion of the distribution of roles and responsibilities in the context of information security management. There are several promising avenues for future work related to the presented generic control management cycle.

Within the scope of the COSEMA project, we develop a comprehensive framework for the IT-based improvement of the communication and coordination among the groups and individuals involved in information security management in general. Having a good understanding of the actual distribution of roles and responsibilities related to control management is considered an essential requirement for that.

The POSECCO project, which also partially funded the research associated with this paper, focuses on the automation of cost-intensive and error-prone activities related to security control management in cross-organizational settings in which one organization has to make sure and prove that it meets security and compliance requirements imposed by other organizations. For that, an extended version of the control management cycle, incorporating not only additional organizational but also external groups and individuals involved in control management such as customers, suppliers and external auditors is considered a valuable artefact.

Beyond that, it could also be worthwhile to investigate the extent to which good practice collections or standards influence organizations in shaping their management of security controls, the issues that arise when they are applied and how they are resolved, as well as under what conditions organisations change, extend or even go beyond established good practice collections and standards.

ACKNOWLEDGMENT

The research associated with this paper was partially funded by the COSEMA project which is sponsored by the Tyrolean business development agency (Standortagentur Tirol) as part of the Translational Research program and the POSECCO project (no. 257129) which is supported by the European Union under the 7th Framework Programme.

REFERENCES

- Anderson, J. A., & Rachamadugu, V. (2006). Information security guidance for enterprise transformation. *Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference*. Hong Kong, China.
- Baker, W. H., & Wallace, L. (2007). Is information security under control? Investigating quality in information security management. *IEEE Security & Privacy*, 5(1), 36-44.
- Barnard, L. & von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls. *Computers & Security*, 19(2), 185-194.
- Böhmer, W. (2008). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. *Proceedings of the 2nd International Conference on Emerging Security Information, Systems and Technologies*. Cap Esterel, France.
- Brykczynski, B. & Small, B. (2003). Securing your organization's information assets. *The Journal of Defense Software Engineering*, 16(5), 12-16.
- Deming, W.E. (1986). *Out of the Crisis*. Cambridge, USA: MIT Press.
- Dhillon, G. & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM*, 43(7), 125-128.
- Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4), 377-397.
- Höne, K., & Eloff, J. H. P. (2002). Information security policy – What do international information security standards say? *Computers & Security*, 21(5), 402-409.
- ISO/IEC. (2005). *Information Technology - Security Techniques - Information Security Management Systems – Requirements (ISO/IEC 27001)*.
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis*. Thousand Oaks, USA: Sage Publications.
- NIST. (2008). *Guide for Assessing the Security Controls in Federal Information Systems (Special Publication 800-53A)*. Retrieved November 6, 2011, from: <http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf>.
- OECD. (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (Recommendation of the OECD Council). Retrieved November 6, 2011, from: <http://www.oecd.org/dataoecd/16/22/15582260.pdf>.
- Patton, M. Q. (1990). *Qualitative Evaluation and Research Methods*. Newbury Park, USA: Sage Publications.
- Shewhart, W. A. (1939). *Statistical Method from the Viewpoint of Quality Control*. Washington, USA: Graduate School of the Department of Agriculture.
- Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-risk management: Technical and insurance controls for enterprise-level security. *Information Systems Security*, 11(4), 33-49.
- Tudor, J. K. (2001). *Information Security Architecture*. Boca Raton, USA: Auerbach Publications.
- von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23, 371-376.