Security Management in Cross-Organizational Settings: A Design Science Approach

Research-in-Progress

Stefan Thalmann
University of Innsbruck
School of Management
Innsbruck, Austria
stefan.thalmann@uibk.ac.at

Daniel Bachlechner
University of Innsbruck
School of Management
Innsbruck, Austria
daniel.bachlechner@uibk.ac.at

Ronald Maier
University of Innsbruck
School of Management
Innsbruck, Austria
ronald.maier@uibk.ac.at

Abstract

The challenges of managing security have increased substantially with the advent of outsourcing and cloud computing. Service providers need to ensure that security controls correctly address the complex sets of requirements demanded by their clients. Auditors find it difficult to check whether service providers are compliant with standard security guidelines as well as organization-specific security requirements. This paper reports research-in-progress of a design science project that addresses security management in cross-organizational settings. Based on a sequence of empirical studies involving interviews and an online survey, we analyze critical activities associated with security management in cross-organizational settings from the perspective of service providers and auditors and discuss the support provided by software. The paper also lays out our plans for developing design artifacts and the theoretical framework for their evaluation.

Keywords: Information security/privacy, design science, IT outsourcing

Introduction

Meeting security requirements is a fundamental issue for organizations operating in an increasingly connected digital economy (Gordon et al. 2010). Organizations are confronted with different sets of security guidelines – both standard (Höne and Eloff 2002) and organization-specific (Siponen and Willison 2009) – which they are required to enforce consistently (Von Solms 2005). This is particularly true for cross-organizational settings in which organizations provide critical services to external parties or consume such services from external parties. Managing security is no longer confined to organization-internal services, systems or infrastructures but has to take into account complex sets of requirements from customers (Currie and Seltsikas 2001). Furthermore, the auditing of security-related processes has become as important as ensuring that effective controls are in place (Kwon and Johnson 2011), but providing evidence that security requirements are properly addressed is considerably more challenging in cross-organizational than in in-house settings (Thalmann et al. 2012).

This paper presents the intermediate results of a design science project that set out to understand and partially automate critical, currently manually-performed and thus error-prone activities of security management in cross-organizational settings. The paper is structured as follows: First, we analyze the research problem in more detail. Next, we present the procedure and intermediate results of a series of empirical studies which yield descriptions of critical activities that were analyzed from the perspectives of service providers and auditors. Using a sequential design (Mingers 2001), a qualitative interview study informed a subsequent quantitative online survey. Then, we analyze the relevance, potential and design characteristics of software support associated with security management in cross-organizational settings. Finally, we discuss the concrete steps planned for the crafting of design artifacts, including a theoretical framework for their evaluation and conclude with a summary of our main findings and plans for this research-in-progress.

Research Problem

Outsourcing of information technology (IT) has a long tradition and started in the 1960s and 1970s (Lee et al. 2003), with companies having gradually outsourced parts of their IT to professional service providers (Lee et al. 2003). More recently, organizations adopted cloud computing (Vouk 2008) which provides software, platforms and infrastructure as services. The steadily increasing number of organizations consuming services out of the cloud is suggestive of this trend (Kaufman 2010). Ensuring that concerns about security are addressed and security requirements are met has become an integral requirement for outsourcing (Khalfan 2004) but is a costly undertaking, involving a considerable amount of manual work.

Common security needs of organizations regardless of size, sector and setting are laid out in information security management guidelines, such as GMITS, COBIT or the IT Baseline Protection Catalogs which describe standard security requirements (Höne and Eloff 2002). Proving compliance with such guidelines and enforcing their consistent application have become central concerns for organizations (Von Solms 2005). Organizations also need to consider their idiosyncratic positions and specify their unique organization-specific security requirements matching their business activities (Siponen and Willison 2009) as well as an increasing number of laws and regulations, e.g., HIPAA or SOX. Managing controls suitable for addressing the diverse range of security needs has become particularly challenging for service providers who are faced with a larger set of requirements than other organizations (Currie and Seltsikas 2001). Auditors are entrusted with checking whether the complex IT landscapes of services providers meet the complex sets of standard and organization-specific security requirements that their clients have to comply with (Hall and Liedtka 2007). This is especially true for clients which need assurance that their financial reports are not adversely affected by inadequately addressed security issues (Julisch et al. 2011).

Simply applying security management procedures from in-house to cross-organizational settings entails several shortcomings. Contracts between service providers and their clients have emerged as a key issue (Saunders et al. 1997). It is not uncommon to see that attempts are made to reduce coordination costs by paying attention to contract details and by designing tighter contracts (Costa 2001). However, controlling technical contract details in complex distributed settings, which take into account the different requirements of all parties to the contract, can be challenging: (1) clients need to be assured that services meet their security requirements, (2) service providers have to cope with numerous individual security requirements, and (3) auditors have to attest and monitor these requirements (Julisch and Hall 2010). As it is impossible to spell out every potential scenario ex-ante, interactions often go beyond specified agreements, and the parties additionally have to rely on mutual trust, commitment and shared interest (Lee et al. 2003).

Organizations entrusted with auditing tasks usually operate in complex and dynamic environments, particularly in the context of cross-organizational settings. Complexity in this area is a consequence of the high number of heterogeneous components interacting in IT landscapes, as well as more and more detailed regulatory and contractual obligations. Both security requirements resulting from regulatory and contractual obligations and IT landscapes are in constant flux leading to uncertainty. Organizational information processing theory (Galbraith 1974) hypothesizes that organizations develop buffers or implement improved information processing capability to reduce the effects of uncertainty (Premkumar et al. 2005). As improved information processing capability has not yet been developed for security management in cross-organizational settings, tool support seems insufficient and a high degree of manual work is currently unavoidable. Designing, implementing and auditing controls are fundamental but error-prone activities. The research problem we address in this paper can be summarized in the question: How can software support the design and verification of security controls in cross-organizational settings?

Software solutions for automating or supporting security management have received considerable attention from the academic community over the last decade. The literature has addressed various aspects and provides a discussion of requirements (Tsoumas and Tryfonas 2004) and design guidelines (Jaferian et al. 2008) for security management solutions, evaluations of the extent of security management automation, both from a technical standpoint (Montesino and Fenz 2011) and from a human and social standpoint (Edwards et al. 2007), and a review of issues related to the automation of specific security management activities (Tracy 2007). Additionally, security management solutions with varying degrees of comprehensiveness were developed and documented (Barruffi et al. 2001; Vermeulen and Von Solms 2002). Research related to security in cross-organizational settings focused, so far, mainly on security issues in IT outsourcing projects (Khalfan 2004), along supply chains (Kolluru and Meredith 2001; Williams et al. 2008) and in networks of organizations (Pulkkinen et al. 2007). Design theory has already proven useful for research on developing secure information systems (Siponen and Baskerville 2006), improving risk management methods (Papadaki and Polemi 2007) and including social and organizational aspects in security management (Monfelt et al. 2011). This paper reports on the current progress of a design science project which develops software set out to assist critical security management activities within the increasingly complex and dynamic environment of cross-organizational settings. The software aims at avoiding or reducing manual work that currently hampers the reaping of the full potential benefits of outsourcing and cloud computing.

Procedure and Intermediate Results

The relevance of information systems (IS) research is directly related to its applicability in designing IT artifacts (Iivari 2007; March and Smith 1995; Peffers et al. 2007). Empirically-based IS concepts and theories should be implementable, and they should synthesize an existing body of research or stimulate critical thinking among IS practitioners (Benbasat and Zmud 1999). The fundamental principle of design science research is that knowledge of a design problem and its solution are acquired in the creation and application of design artifacts (Hevner et al. 2004) such as constructs, models, methods and instantiations (March and Smith 1995). The outcome of this type of research is not only the design artifact itself but also a clearly defined contribution to scientific knowledge (Hevner et al. 2004; Kuechler and Vaishnavi 2008; Ricciardi and De Marco 2011). Theorizing and theory building are present in all phases of design science (Venable 2006). Consequently, design propositions created in rigorous design science research need to be tested empirically and grounded in theory (Carlsson 2007; Iivari 2007).

A review of theories can suggest new research hypotheses and guide their evaluation (Nunamaker et al. 1991). Deficits of or possibilities for improving theories are often detected during design (Nunamaker et al. 1991; Purao et al. 2008). Even where (designed) solutions work well, often, very little is known about why or how they work (Ricciardi and De Marco 2011). Therefore, design science investigates design artifacts as well as their implementation context by referring to pre-existing theories (Venable 2006). Baskerville et al. (2011) distinguish (1) designing with research, i.e. to achieve a good design focusing on domain knowledge, (2) research into design, i.e. to understand the design activity focusing on design process knowledge and (3) design as research methodology, i.e. to understand the scope of research, focusing on domain knowledge. As a result, design science research should create precise statements about the knowledge so that it can contribute to design as well as to domain theories (Baskerville et al. 2011; Ricciardi and De Marco 2011). The context of design and use is critical in IS, considering it is a socio-technical discipline (McKay and Marshall 2005). Hence, design science research not only focuses on the technology-oriented design artifacts but also needs to consider the solution's socio-economic implementation context (Carlsson 2007).

We structure our research according to three interacting cycles (Hevner 2007). The relevance cycle bridges the environment with the actual design activities to define the research goal, justify the value of the solution and show its relevance to the application domain (Peffers et al. 2007). During requirements elicitation, particular attention is also paid to measuring the improvement made. The rigor cycle identifies the scientific contribution of the design science work (Hevner 2007), using theories to guide the evaluation and explain its results (March and Smith 1995), and communicates the results to the scientific community (Peffers et al. 2007). The design cycle represents the core activity of design science, to build and evaluate (March and Smith 1995), i.e. artifacts are created based on the requirements from the relevance cycle and evaluated based on the insights gained from the rigor cycle (Hevner 2007). Applied to the security management context, the resulting design artifact should not only contribute to practice but also to the scientific knowledge base by improving the current understanding of security management in cross-organizational settings. Figure 1 illustrates the steps performed so far and our intermediate results which we describe in the following. Note that while the cycles are interconnected, they are not necessarily implemented in sequence.

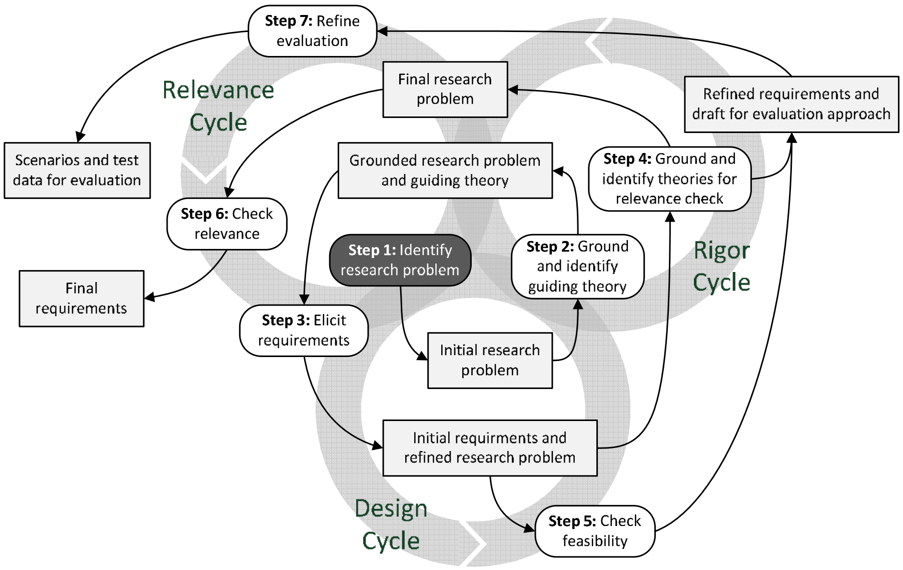
Step 7: Refine evaluation
Final research problem
Refined requirements and draft for evaluation approach
Relevance Cycle
Scenarios and test data for evaluation
Grounded research problem and guiding theory
Step 4: Ground and identify theories for relevance check
Step 6: Check relevance
Step 1: Identify research problem
Step 2: Ground and identify guiding theory
Rigor Cycle
Final requirements
Step 3: Elicit requirements
Initial research problem
Initial requirments and refined research problem
Design Cycle
Step 5: Check feasibility

Figure 1. Research Procedure and Intermediate Results

Step 1: Identify the Research Problem

We developed our research problem based on the actual business needs of a service provider and an auditor, who were joint partners in a research project involving academia and industry. At the start, both application partners sketched out their expectations with respect to tool support for cross-organizational security management. By first analyzing the sketches and further exploring these expectations in two semi-structured, face-to-face interviews, we were able to formulate the initial research problem. The resulting research problem can be characterized as "wicked" (Rittel and Webber 1973) on the basis of the following features: (1) an ill-defined environmental context, i.e. complex IT landscapes and risk assessments that critically depend upon human, social and cognitive abilities, (2) complex interactions among sub-components as controls are interdependent and can contradict each other, and (3) inherent flexibility in response to frequent changes in the security requirements and in the IT landscapes.

Step 2: Ground and Identify the Guiding Theory

We grounded the initial research problem in the body of literature. The revised IS participation theory (Markus and Mao 2004) methodologically guided our activities related to the relevance cycle. The theory hypothesizes a link between users participating in design activities and the success of development and implementation. Selecting users is critical, especially where only a small subset of users can participate in the design activities. A stakeholder approach is recommended to investigate the design problem in detail (Markus and Mao 2004). Consequently, we decided to perform a participatory design approach (Butler and Fitzgerald 1997) whereby we involve carefully selected key stakeholders of our application partners more participatory. Both design artifacts and the implemented solution will be evaluated using constructs associated with IS participation theory, thus subdividing system success into, on the one hand, its design and on the other, its implementation success (Markus and Mao 2004).

Step 3: Elicit Requirements

We investigated the relevance of the research problem, including its underlying activities, current tool support and involvement of key stakeholders, and gathered concrete requirements for software support; then, we created a first draft of the criteria for measuring improvement (Hevner 2007) in 14 semi-structured, one-hour long telephone interviews. The experienced key stakeholders who were interviewed between January and May 2011 represented three service providers, three service consumers and two auditors. While twelve interviews were recorded and transcribed, the interviewers took notes and produced written summaries immediately after conducting the other two interviews. The purposeful sample included practitioners such as security managers, operations managers or auditors involved in cross-organizational security management. The qualitative data was analyzed by classifying chunks of text into meaningful codes (Miles and Huberman 1994). In the following, we describe three critical activities to be supported and for each of these activities we discuss the key stakeholders involved, tool support, the related claim and the evaluation criteria for assessing the achievement of the claim.

Select Control Objectives

Auditors select control objectives supported by senior managers from their clients, considering their security requirements as well as their IT landscape. As not everything can be fully controlled, some risks need to be selected on the basis of their relevance and measurability. Auditors identify critical business processes by interviewing their clients' business experts and by analyzing documents as part of defining the audit scope. Then, relevant control objectives are selected, taking the clients' IT landscapes into account. The key stakeholders involved in this activity are internal and external auditors, and, where services are outsourced, also the supplier relationship manager. The activity is currently not comprehensively supported by tools. Our interviewees reported that only individually designed spreadsheets and other standard office products are used. Auditors usually follow guidelines provided by their company. According to one auditor, "there is currently no tool support, it is just interviewing". Auditors mentioned an apparent lack of tool support which becomes more critical with the increasing complexity. Particularly in cross-organizational settings, selecting control objectives is often costly and the quality of the results heavily relies on the business experts' willingness to cooperate.

We claim that the selection of control objectives can be improved by collecting and aggregating data required for audit scoping with the help of formal models of critical business processes and IT landscapes. To assess our claim, we propose the following criteria: (1) time to perform the audit scoping and (2) number of employees involved.

Design Controls

Controls need to be designed in such a way that they are able to address the risks identified when selecting control objectives, taking into account controls already implemented, current IT landscapes, performance and cost issues as well as feasibility of implementation. Simulations of the impacts of planned controls are able to check whether control objectives are covered by controls and whether negative side effects can be expected. Control design relies heavily on the experience and intuition of the individuals involved due to the highly complex IT landscapes and the lack of tool support. An internal auditor stated that "usually changes need to be performed fast and hence only with a few tests – which then can result in errors". Auditors check if a control design meets the control objectives during audits. Internal auditors, security managers and systems architects are primarily responsible for designing controls.

We claim that the control design can be improved by showing which control objectives are covered by the existing controls, and which further controls are needed. Criteria for assessing our claim are (1) time to check whether controls meet specific control objectives, (2) time to select a control meeting a specific requirement, (3) number of configurations considered and (4) number of employees involved.

Verify Control Implementations

The defined set of controls needs to be implemented so that it operates effectively and meets the control objectives. The IT landscape has to be configured accordingly and the impact on the existing control set needs to be checked beforehand. Our solution focuses on verifying these activities. Organizations need to gain assurance on the effectiveness of their own and their suppliers' controls. Typically, auditors are entrusted to perform suitable checks. Particularly service providers need to verify their control implementation in defined time intervals to prevent security incidents and to be considered trustable parties. Simulations are used to check the system configuration against some test cases. The challenge here is to manage the fast changing environment and the changing sets of controls. Within the scope of the interviews, an auditor explained that deficiencies are "related to the complexity of the technology, because it's moving a lot […] we are not able to follow and we don't have appropriate ways to test the effectiveness of controls". The systems architect, the security manager and IT professionals are engaged with service providers in implementing controls and regularly assessing the landscape's integrity. The verification of the control implementation is an essential part of an auditor's activities.

We claim that the verification of control implementations can be improved by assessing whether a configuration of elements of an IT landscape effectively implements a control design. To assess our claim, we propose the following criteria: (1) time to detect security misconfigurations in a specific landscape, (2) time to anticipate the impact of a specific change, (3) number of relevant security misconfigurations detected in a specific landscape and (4) number of employees involved.

Step 4: Ground and Identify the Theories for the Relevance Check

The results of the stakeholder-based requirements elicitation also need to be grounded in theory. We identified approaches suitable to meet the requirements in a literature review and also checked approaches, procedures and tools mentioned by the stakeholders. However, we came to the conclusion that existing approaches like auditing guidelines and spreadsheet applications can only be applied to small sub-problems. No single tool or collection of tools covers the entire spectrum of requirements. Thus, the requirements were revised accordingly. Since the survey participants were potential users of our software, we selected user involvement in activities as construct (Barki and Hartwick 1994; Hartwick and Barki 1994) which is defined as an attitude towards a new system and refers to the extent to which an individual believes that a new system is important and personally relevant. The second aspect was the current support provided by software which we use in the quantitative study performed in step 6.

Step 5: Check Feasibility

We identified first drafts for evaluation criteria which can be used to measure the improvements of the intended software on the stakeholders' activities. The design team then checked the feasibility of the formulated requirements and the suitability of the evaluation criteria and revised them accordingly. We refined our claims using performance metrics (Hevner et al. 2004). Functional requirements were formulated for the three selected activities. Our software enables a formal description of the organizational IT landscape, its risks and critical business processes as well as reports which can be used for selecting control objectives including a check whether control objectives contradict each other. For designing controls, the software provides an overview of which controls cover what control objectives together with additional information according to pre-specified dimensions. It allows checking the equivalence of controls, to anticipate the impact of changes and to check if a new control covers a control objective in a specific IT landscape. Concerning the verification of control implementations, the software performs simulations to check whether the configuration of the IT landscape is correct regarding the designed controls upon request as well as continuously with an alert function in case of misconfigurations.

Step 6: Check Relevance

We investigated the relevance of the identified activities in a questionnaire-based anonymous online survey between December 2011 and March 2012 using a larger snowball sample of experts. General explanations as well as survey questions contained language similar to the one used by the interviewees in the qualitative study. Graphical illustrations were used so that the activities were self-explanatory. As described in step 4, we checked the user involvement and the current software support for the identified activities. The software support was only checked if participants personally performed an activity at least once a year and hence not every participant answered every question. In all, 134 questionnaires were sufficiently completed, and as they were free of anomalies, they could be used for the analysis. The survey instrument was pre-tested with 33 experts, resulting in revisions of the questionnaire, specifically with regards to the presentation of activities and functional requirements.

Figure 2 presents the results. The scales range from 1 - low to 7 - high involvement and from 1 - bad to 7 - good software support. The majority of the survey participants are highly involved in the activities, yet also rate the current software support as bad, supporting the relevance of our claims. Participants were also requested to list software they used to perform the activities. Spreadsheet applications were mentioned most often, however, none of the software fulfilled the identified requirements.

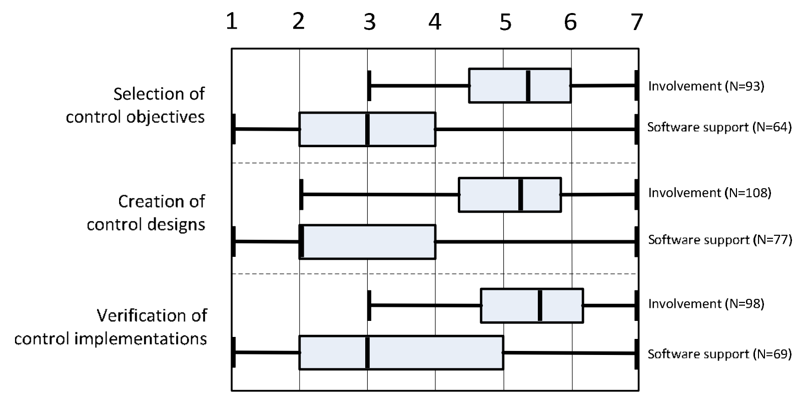

Figure 2. Results of the Quantitative Relevance Check

Step 7: Refine the Evaluation

Design science artifacts need to be assessed whether they improve criteria of value or utility (March and Smith 1995). IT artifacts are always related to action and effect as they are designed, constructed and used by humans (Orlikowski and Iacono 2001). Evaluating design artifacts and their impact thus needs to consider humans and their context (Basili 1996) and the efforts required for applying empirical methods (Hevner et al. 2004) which involve a large number of variables and human actors that can affect the result. However, ignoring organizational context and human perspective would in many cases mean oversimplification (Basili 1996). In our case, a controlled experiment seems appropriate with clearly defined activities carried out by subjects that perform these activities in their jobs based on data taken from real organizational settings thereby reducing the number of confounding variables. We specified the evaluation in coordination with our key stakeholders involved in the design activities, including suitable evaluation scenarios and test data. The performance of test cases related to the scenarios will first be assessed without, then with software support and compared using the pre-defined evaluation criteria.

Discussion

So far, we concentrated on the relevance cycle and developed the research problem. We identified key activities which are critical for cross-organizational security management. All of these can also be performed in traditional in-house settings. However, the complexity of these activities is higher as a result of the involvement of several parties, causing disproportionately high efforts when performed manually. Service providers are also faced with frequent changes of security requirements and hence need to perform these activities frequently, further stressing the relevance of software support which is currently considered weak by our survey participants. This underpins our design goal of creating software to improve these activities. A multi-method approach was chosen based on the premise that separate and dissimilar data sets collected on the same phenomena would provide a richer picture (Sawyer 2001). The combination of qualitative and quantitative methods, i.e. a qualitative interview study and a subsequent quantitative online survey in a sequential design (Mingers 2001), not only provided a rich context but also allowed to take into account a considerable number of opinions (Kaplan and Duchon 1988).

In the next steps, the project will focus on the design cycle and the rigor cycle. In step 8, we will create the main design artifact supporting the identified key activities of cross-organizational security management. In parallel, in step 9, we will select and operationalize a theoretical framework supporting the evaluation of our design artifact. The goal is to provide explanations for why and how the underlying activities are affected by the solution. Insurance theory (Marshall 1974) can provide the foundation for selecting control objectives. The theory focuses on the assessment of risks and the design of insurance contracts as well as on the effects of insurance on individuals. The implementation of controls has many similarities with an insurance contract. It takes into account future impact expectation (especially on financial measures) as well as costs for implementing and monitoring controls. A future contribution of our research to scholarly knowledge can be expected from the investigation of how the audit scope changes if monitoring and checking of controls can be automated or supported.

Similarly, management control theory (Koontz 1959) discusses the control definition process, its implementation and the determination of standards in organizational contexts and can be used to transfer insights from designing and implementing management controls to the domain of IT controls. Here, a future contribution to scholarly knowledge can be expected from the investigation of how the process of control design and implementation changes if it can be automated or supported. An in-depth understanding of the relevant concepts and relationships can be expected through the instantiation of management control theory in the domain of IT controls. In step 10, we will evaluate the main design artifact and assess our claims based on the proposed evaluation criteria. Particular emphasis will be placed on the artifact's impact on the problem domain. Steps 8 and 10 will be performed repeatedly to refine the design artifact (Hevner 2007) until a satisfactory design is achieved. We further plan to reflect on our findings and artifacts in the light of similar contexts such as supply chains.

Summary

Within the scope of this research-in-progress paper, we specified a research problem in security management which arises from highly complex and dynamic security requirements and IT landscapes in cross-organizational settings. Within a series of empirical studies, we investigated this research problem and identified three key activities, namely, selecting control objectives, designing controls and verifying control implementations. Our findings indicate that these activities are currently not well supported by software. We concretized the corresponding demand for tool support through the development of a set of evaluation criteria which can be used to assess the impact of our solution on these activities. So far, we specified the research problem, assessed its relevancy and identified criteria which can be used to assess its impact. The next steps will be to build software on the basis of the requirements identified and to evaluate it rigorously.

Acknowledgments

The research leading to the presented results was partially funded by the European Commission under the 7th Framework Programme (FP7) through the PoSecCo project (project no. 257129).

References

Barki, H., and Hartwick, J. 1994. "Measuring User Participation, User Involvement, and User Attitude," Management Information Systems Quarterly (18:1), pp. 59-82.

Barruffi, R., Milano, M., and Montanari, R. 2001. "Planning for Security Management," IEEE Intelligent Systems (16:1), pp. 74-80.

Basili, V.R. 1996. "The Role of Experimentation in Software Engineering: Past, Current, and Future," 18th Int. Conf. Software Eng., Los Alamitos, Calif.: IEEE Computer Soc. Press.

Baskerville, R.L., Kaul, M., and Storey, V.C. 2011. "Unpacking the Duality of Design Science," in: Thirty Second International Conference on Information Systems. Shanghai, Paper 10.

Benbasat, I., and Zmud, R.W. 1999. "Empirical Research in Information Systems: The Practice of Relevance," Management Information Systems Quarterly (23:1), pp. 3-16.

Butler, T., and Fitzgerald, B. 1997. "A Case Study of User Participation in the Information Systems Process," 18th International Conference on Information Systems, Atlanta, pp. 411-426.

Carlsson, S.A. 2007. "Developing Knowledge through IS Design Science Research," Scandinavian Journal of Information Systems (19:2), Article 2.

Costa, C. 2001. "Information Technology Outsourcing in Australia: A Literature Review," Information Management & Computer Security (9:5), pp. 213 - 224.

Currie, W., and Seltsikas, P. 2001. "Exploring the Supply-Side of IT Outsourcing: The Emerging Role of Application Service Providers," European Journal of Information Systems (10:3), pp. 123-134.

Edwards, W.K., Poole, E.S., and Stoll, J. 2007. "Security Automation Considered Harmful?," in: Workshop on New Security Paradigms NSPW '07. ACM, pp. 33-42

Galbraith, J.R. 1974. "Organization Design: An Information Processing View," Interfaces (4:3), pp. 28-36.

Gordon, L.A., Loeb, M.P., and Sohail, T. 2010. "Market Value of Voluntary Disclosures Concerning Information Security," Management Information Systems Quarterly (34:3), pp. 567-594.

Hall, J.A., and Liedtka, S.L. 2007. "The Sarbanes-Oxley Act: Implications for Large-Scale IT Outsourcing," Communications of the ACM (50:3), pp. 95–100.

Hartwick, J., and Barki, H. 1994. "Explaining the Role of User Participation in Information System Use," Management Science (40:4), pp. 440-465.

Hevner, A.R. 2007. "A Three Cycle View of Design Science Research," Scandinavian Journal of Information Systems (19:2), pp. 87-92.

Hevner, A.R., March, S.T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," Management Information Systems Quarterly (28:1), pp. 75-105.

Höne, K., and Eloff, J.H.P. 2002. "Information Security Policy — What Do International Information Security Standards Say?," Computers & Security (21:5), pp. 382-475.

Iivari, J. 2007. "A Paradigmatic Analysis of Information Systems as a Design Science," Scandinavian Journal of Information Systems (19:2), Article 5.

Jaferian, P., Botta, D., Raja, F., Hawkey, K., and Beznosov, K. 2008. "Guidelines for Designing IT Security Management Tools," in: 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology San Diego, CA, USA ACM, Article 7.

Julisch, K., Suter, C., Woitalla, T., and Zimmermann, O. 2011. "Compliance by Design - Bridging the Chasm between Auditors and IT Architects," Computers & Security (30:6-7), pp. 410-426.

Kaplan, B., and Duchon, D. 1988. "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study," Management Information Systems Quarterly (12:4), pp. 571-586.

Kaufman, L. 2010. "Can Public-Cloud Security Meet Its Unique Challenges?," IEEE Security&Privacy (8:4), pp. 55-57.

Khalfan, A.M. 2004. "Information Security Considerations in IS/IT Outsourcing Projects: A Descriptive Case Study of Two Sectors," International Journal of Information Management (24:1), pp. 29-42.

Kolluru, R., and Meredith, P.H. 2001. "Security and Trust Management in Supply Chains," Information Management & Computer Security (9:5), pp. 233-236.

Koontz, H.D. 1959. "Management Control: A Suggested Formulation of Principles," California Management Review (1:2), pp. 47-55.

Kuechler, B., and Vaishnavi, V. 2008. "On Theory Development in Design Science Research: Anatomy of a Research Project," European Journal of Information Systems (17), pp. 489–504.

Kwon, J., and Johnson, M.E. 2011. "The Impact of Security Practices on Regulatory Compliance and Security Performance," Thirty Second International Conference on Information Systems, Shanghai.

Lee, J.N., Huynh, M.Q., Kwok, R.C., and Pi, S.M. 2003. "IT Outsourcing Evolution: Past, Present, and Future," Communications of the ACM (46:5), pp. 84-89.

March, S., and Smith, G. 1995. "Design and Natural Science Research on Information Technology," Decision Support Systems (15:4), pp. 251-266.

Markus, M.L., and Mao, J. 2004. "Participation in Development and Implementation - Updating an Old, Tired Concept for Today's IS Contexts," Journal of the Association for Information Systems (5:11-12), pp. 514-544.

Marshall, J.M. 1974. "Insurance Theory: Reserves Versus Mutuality," Economic Inquiry (12:4), pp. 476-492.

McKay, J., and Marshall, P. 2005. "A Review of Design Science in Information Systems," in: 16th Australasian Conference on Information Systems. Sydney, Australia: Paper 5.

Miles, M.B., and Huberman, A.M. 1994. Qualitative Data Analysis: An Expanded Sourcebook, (2nd ed.). Thousand Oaks, CA: Sage.

Mingers, J. 2001. "Combining IS Research Methods: Towards a Pluralist Methodology," Information Systems Research (12:3), pp. 240 - 259.

Monfelt, Y., Pilemalm, S., Hallberg, J., and Yngström, L. 2011. "The 14-Layered Framework for Including Social and Organizational Aspects in Security Management," Information Management & Computer Security (19:2), pp. 124-133.

Montesino, R., and Fenz, S. 2011. "Information Security Automation: How Far Can We Go?," in: Sixth International Conference on Availability, Reliability and Security. Vienna, Austria: IEEE, pp. 280-285.

Nunamaker, J.F., Chen, M., and Purdin, T.D.M. 1991. "Systems Development in Information Systems Research," Journal of Management Information Systems (7:3), pp. 89-106.

Orlikowski, W.J., and Iacono, C.S. 2001. "Research Commentary: Desperately Seeking "IT" in IT Research - a Call to Theorizing the IT Artifact," Information Systems Research (12:2), pp. 121-134.

Papadaki, K., and Polemi, N. 2007. "Towards a Systematic Approach for Improving Information Security Risk Management Methods " in: 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. Athens, Greece: IEEE.

Peffers, K., Tuunanen, T., Rothenberger, M.A., and Chatterjee, S. 2007. "A Design Science Research Methodology for Information Systems Research," Journal of Management Information Systems (24:3), pp. 45 - 77.

Premkumar, G., Ramamurthy, K., and Saunders, C.S. 2005. "Information Processing View of Organizations: An Exploratory Examination of Fit in the Context of Interorganizational Relationships," Journal of Management tnformation Systems (22:1), pp. 257-294.

Pulkkinen, M., Naumenko, A., and Luostarinen, K. 2007. "Managing Information Security in a Business Network of Machinery Maintenance Services Business – Enterprise Architecture as a Coordination Tool," The Journal of Systems and Software (80:10), pp. 1607–1620.

Purao, S., Baldwin, C., Hevner, A., Storey, V.C., Pries-Heje, J., Smith, B., and Zhu, Y. 2008. "The Sciences of Design: Observations on an Emerging Field," Communications of the Association for Information Systems (23:1), Article 29.

Ricciardi, F., and De Marco, M. 2011. "Extracting Knowledge from within Design Processes: An Emerging Issue for IS Research," in: 6th Mediterranean Conference on Information Systems. Limassol Cyprus: Paper 34.

Rittel, H.W.J., and Webber, M.M. 1973. "Dilemmas in a General Theory of Planning," Policy Sciences (4:2), pp. 155-169.

Saunders, C., Gebelt, M., and Hu, Q. 1997. "Achieving Success in Information Systems Outsourcing," California Management Review (39:2), pp. 63-79.

Sawyer, S. 2001. "Analysis by Long Walk: Some Approaches to the Synthesis of Multiple Sources of Evidence," in Qualitative Research in IS: Issues and Trends, E.M. Trauth (ed.). Hershey, PA: IDEA pp. 163-189.

Siponen, M., and Baskerville, R.L. 2006. "A Design Theory for Secure Information Systems Design Methods," Journal of the Association for Information Systems (7:11), pp. 725-770.

Siponen, M., and Willison, R. 2009. "Information Security Management Standards: Problems and Solutions," Information & Management (46:5), pp. 267–270.

Thalmann, S., Bachlechner, D., Demetz, L., and Maier, R. 2012. "Challenges in Cross-Organizational Security Management," 45th Hawaii International Conference on System Sciences (HICSS), R.H. Sprague (ed.), Grand Wailea, Maui, USA: IEEE Computer Society, pp. 5480-5489.

Tracy, R.P. 2007. "IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards," Information Systems Security (16:2), pp. 114–122.

Tsoumas, V., and Tryfonas, T. 2004. "From Risk Analysis to Effective Security Management: Towards an Automated Approach," Information Management & Computer Security (12:1), pp. 91-101.

Venable, J.R. 2006. "The Role of Theory and Theorising in Design Science Research," in: First International Conference on Design Science Research in Information Systems and Technology. Claremont, CA: pp. 1–18.

Vermeulen, C., and Von Solms, R. 2002. "The Information Security Management Toolbox - Taking the Pain out of Security Management," Information Management & Computer Security (10:3), pp. 119-125.

Von Solms, S.H. 2005. "Information Security Governance - Compliance Management Vs Operational Management," Computers & Security (24:6), pp. 443-447.

Vouk, M.A. 2008. "Cloud Computing: Issues, Research and Implementations," Journal of Computing and Information Technology (16:4), pp. 235-246.

Williams, Z., Lueg, J.E., and LeMay, S.A. 2008. "Supply Chain Security: An Overview and Research Agenda," The International Journal of Logistics Management Information Systems Quarterly (19:2), pp. 254-281.