Using Stakeholder Knowledge for Data Quality Assessment in IS Security Risk Management Processes

Christian Sillaber
University of Innsbruck
Technikerstrasse 21a
6020 Innsbruck
christian.sillaber@uibk.ac.at

Ruth Breu
University of Innsbruck
Technikerstrasse 21a
6020 Innsbruck
ruth.breu@uibk.ac.at

ABSTRACT

The availability of high quality documentation of the IS as well as knowledgeable stakeholders are an important prerequisite for successful IS security risk management processes. However, little is known about the relationship between stakeholders, their knowledge about the IS, security documentation and how quality aspects influence the security and risk properties of the IS under investigation. We developed a structured data quality assessment process to identify quality issues in the security documentation of an information system. For this, organizational stakeholders were interviewed about the IS under investigation and models were created from their description in the context of an ongoing security risk management process process. Then, the research model was evaluated in a case study. We found that contradictions between the models created from stakeholder interviews and those created from documentation were a good indicator for hidden security risks. The findings indicate that the proposed data quality assessment process provides valuable inputs for the ongoing security and risk management process. While current research considers users as the most important resource in security and risk management processes, little is known about the hidden value of various entities of documentation available at the organizational level. This study highlights the importance of utilizing existing IS security documentation in the security and risk management process and provides risk managers with a toolset for the prioritization of security documentation driven improvement activities.

Keywords

information systems security risk management; information system security documentation quality; data quality of information system security documentation; stakeholder knowledge driven process

1. INTRODUCTION

An increasing number of studies shows that the majority of incidents related to information system security can be traced back to internal stakeholders (e.g. [4, 23, 3]). Over the last years, IS security literature has been constantly moving from portraying users as the weakest link in IS security (e.g. [27, 19]) to viewing them as the solution to multiple IS security issues (e.g. [21, 20, 1]).

Calls for more research in IS security and risk management processes to investigate stakeholders and artifacts created by them in more detail have been frequently made [20, 25, 2, 13, 18]. While many studies followed this call and examined the value provided by stakeholders in IS security and risk management processes, literature is scarce with empirical studies that examine more closely how available artifacts can be utilized in IS security risk management processes.

Based on the premise that, besides focusing on the participation of stakeholders as mere subjects of IS security policies, it is worthwhile to investigate already available artifacts, such as IS security documentation, the present paper's research question asks how, these artifacts can bring value during analysis phases of the IS security and risk management process.

User participation in IS development and its influence on implementational success has been extensively researched and it has been repeatedly argued that the information exchange and knowledge transfer resulting from such participation is the single most important effect [9]. Accordingly, the inclusion of multiple stakeholders in the risk management process has already been included in most established IS security risk management processes [14, 24].

The objective of this paper is to examine the utilization of existing IS security documentation in analysis phases of the IS security risk management processes and to examine how data quality of the documentation impacts the IS security and risk management process. In doing so, this paper answers calls for empirical research on user participation in IS security risk processes [10] and validates the findings in a case study at the organization under investigation. The research presented in this paper generalizes our research on stakeholders' business process awareness and its contribution to an ongoing IS security and risk management process [17].

The remainder of this paper is organized as follows. First, related work on user participation in IS security and risk management settings is presented and an overview on existing state-of the art research is presented. Next, the study's multi-method research design is outlined, followed by a qualitative exploratory study that examined data quality in IS security documentation and its contribution to the IS security and risk management process. A theoretical model informed by IS development theories and the qualitative study is then tested in a confirmatory quantitative study. Finally, the paper concludes with a discussion of the implications of the study, limitations, and suggestions for future research.

2. RELATED WORK

IS security risk management is the continuous process to identify and assess risk and to apply methods to reduce risks to an accept-

SIGMIS-CPR'15, June 4–6, 2015, Newport Beach, CA, USA.

ACM 978-1-4503-3557-7/15/06 ...$15.00.
http://dx.doi.org/10.1145/2751957.2751960.

able extent. Recent research has increasingly focused on human factors influencing the outcome of IS security and risk management processes. Previous research focuses on behavioral theories [1], describing the entire IS security and risk management process, security awareness [20, 11], behavior [6], communication [7] and the positive impact of audits [22] and standardization efforts [12].

Following a synthesis of theories explaining user participation in IS security contexts, Spears et al. [20] define *user participation in information systems security risk management* as the set of behaviors, activities, and assignments undertaken by business users during risk assessment and the design and implementation of IS security controls that is expected to add value to security risk management. By focusing on the *assessment* (i.e. analysis) phase, we re-conceptualize the success outcomes, actors, activities and hypothesized links between outcomes and activities to fit the concepts under investigation in the present paper, as suggested in [20]. Therefore, the present paper examines the link between static artifacts i.e. IS security documentation and activities and the value they add to the overall process.

3. MULTI-METHOD RESEARCH DESIGN

A combination of data collection and analysis methods were used on separate samples to examine data quality in the analysis phase of IS security and risk management processes. In a first step interviews were conducted. Then, in the next step, a qualitative analysis on a different sample of professionals who participated in an organizational IS security and risk management process was conducted.

This multi-method or mixed-method approach was chosen based on the premise that separate and dissimilar data sets would provide a richer picture and thus compensate for the fact that experimentations in IS security and risk management processes are difficult to conduct [8, 26]. A sequential design was used in that the qualitative exploratory study informed a subsequent confirmatory study.

Qualitative methods were appropriate as they provide a rich understanding of the activities, behaviors and assignments that define user participation in the context of this study [8]. Furthermore, they allow for the construction of a framework for analysis. As the theories were used as a framework of analysis, data collection for the qualitative study was not based on any *a-priori* theories and can therefore be considered as an exploratory study.

Quantitative methods were then employed to test the theoretical framework derived from the quantitative study based on the researchers' understanding. Hypotheses that were constructed from the qualitative study formed a model that examined the degree to which data quality of information system security documentation explained variation in pre-specified outcome variables. Thus, combining qualitative and quantitative methods provided both a rich context and testability to the study.

4. EXPLORATORY STUDY

An exploratory study was conducted in two phases to better understand the connection between data quality of information system security documentation and the quality of the IS security and risk management process and to investigate its outcomes.

The first phase of the exploratory study was conducted during an ongoing research project that investigated the efficient management of security requirements at an organization. The organization under investigation is one local branch (Company A; $\approx$ 1200 employees) of a multinational IT service provider, providing various cloud services.

The second phase of the exploratory study, where the findings from the first phase were refined and extended, was conducted during an ongoing action design research project [15] seeking to improve the IS security risk management process currently used by the organization. The organization under investigation is one local branch (Company B; $\approx$ 100 employees) of a multinational engineering company, focusing on the development of distributed information systems within a highly regulated domain.

The remainder of this section describes the data collection and analysis process as well as the findings of the exploratory study.

4.1 Data Collection

To conduct the exploratory study, informants currently involved in the management of security requirements (Company A), or the IS security and risk management process were identified within the organization.

At company A, six interviews were conducted with six informants including one chief security officer, two security managers, one internal auditor and two external auditors. The external auditors were not directly affiliated with company A but closely involved in the aforementioned research project and therefore included to obtain an external view. Each interview lasted between 10 and 90 minutes and the informants were granted anonymity.

At company B, five semi-structured interviews were conducted with five informants including three product managers, one deputy chief information security officer and one technological executive. This convenience sample included three employees with a degree in computer science and one with a specialization in IS security. Each interview lasted approximately 45 minutes and was recorded. The informants were granted anonymity. The interviews were conducted as part of an ongoing action design research project and informants were told the purpose of the study was to gain a better understanding of the fit between business needs and the IS security risk management process.

All informants were asked to recall information on the business security requirements, available documentation, and quality issues related to the system and business processes under investigation in the IS security and risk management process and to identify security requirements and risks accordingly. In parallel, information system security documentation, documentation on the business processes, as well as security guidelines and policy documents were obtained from internal knowledge bases documenting information system development and information system usage.

4.2 Analysis

An iterative process of three manual coding techniques was applied to interview transcriptions. First, selective coding was used to develop an initial code list that contained: attributes of data quality (e.g. *incomplete, not available, outdated*), references to information system security documentation (e.g. specific documents or tools), system components and their link to information system security documentation (e.g. *"Security requirements for component XY can be found in file Z"*) and risks. Next, open-ended coding was used to identify new codes as they emerged from interview transcripts and to identify differences between the two companies. Finally, relationships between information system security documentation data quality, security requirements, stakeholder participation in the IS security and risk management process and risks were identified.

As informants described the information system currently under risk analysis, they were asked which parts of the information system relate to which risks and to describe their knowledge on

different aspects of the available information system security documentation.

Once the data had been collected, segments of interview transcripts were coded as related to information system security documentation data quality when informants recalled specific documents when eliciting risks or security requirements. These coded segments were subsequently grouped and assigned new codes that categorized the activities in which users participated. Relationships among codes were then analyzed. These findings are presented in the next section.

4.3 Results

Informants described their roles and activities in relationship to different parts of the IS under investigation during the IS security and risk management process. They described information system security documentation they were aware of, quality problems related to these documents and processes and workflows that use these documents. Then they described possible contributions of these documents to the IS security and risk management process in terms of identified risks, elicited security requirements and business needs from their perspective. Each of these aspects is described below, providing contextual detail of information system security documentation data quality and the derived benefit to the IS security risk management process.

All informants indicated that they had participated in the past in creating or maintain information system security documentation - at least at an informal level, thus confirming the observations made in [20]. The informants also confirmed, that the information system security documentation that is available at the organization is a main source of information for the IS security and risk management process. Furthermore, all informants (except for the external auditors at company A) stated they have already provided input to past IS security and risk management processes based on their respective domain knowledge.

As for the information system security documentation itself, we could elicit the following classification for data quality:

- **Missing**: the stakeholder could not identify a document related to the security of a specific system component.
- **Incomplete**: the stakeholder could only identify documents that were missing information (e.g. missing documentation of responsible roles). We differentiated between missing documentation and incomplete information system security documentation if a document had at least one reference to the system under investigation.
- **Wrong**: the documents identified by the stakeholder were either contradicting observations made in the system (e.g. outdated information) or were factually wrong (e.g. a non-existing stakeholder was referenced).

Regarding the participation of stakeholders during the risk management process and the information system security documentation used there, stakeholders reported their past involvement during (1) the analysis (2) the risk mitigation strategy creation (3) control design and (4) control implementation phase [20]. The informants reported on their utilization of information system security documentation during all phases.

All informants reported that they felt most confident when asked about areas of the information system where they had complete and correct information system security documentation available. If the available information system security documentation was incomplete or (partially) wrong, stakeholders a) complained about the bad quality, b) asked to consult external sources or c) started an internal change process to improve the documentation. Furthermore, stakeholders expressed the suspicion that the bad data quality might indicate problems with the information system that the documentation should cover. During the ongoing IS security and risk management process at company B, we asked stakeholders to recreate information system security documentation of one specific component as all available documentation was using an informal notation, unsuitable for the IS security and risk management process. During the recreation process (during an on-site workshop) we could observe that the new documents partially contradicted the previous documentation. We could trace back the contradiction to two stakeholders that were responsible for the components with the contradicting security requirement (Mutatis mutandis): Stakeholder 1 relied on stakeholder 2 to implement security controls and stakeholder 2 assumed that the security controls have been implemented by stakeholder 1.

We could observe, that components of the information system under investigation with severe data quality problems were often associated with higher risk levels and ill-defined security requirements during the IS security and risk management process. This observation is further examined in the confirmatory study by testing the hypothesis:

> **H1:** Data quality issues in information system security documentation are an indicator for security problems in corresponding areas of the information system under investigation in an IS security and risk management process.

Informant answers related to the data quality of the available information system security documentation varied largely on the context of use. We observed that stakeholders working in management roles had a different understanding of information system security documentation data quality than the rest of stakeholders. While managerial stakeholders were more concerned with availability and up-to-date information (e.g. in a central knowledge base), other stakeholder were more concerned with completeness of the information. Furthermore, we observed that no concise definition of data quality for information system security documentation existed at both companies. For instance, Anton (name changed for anonymity) a CISO said that: *"I do not know what [good data quality] means in this context, but I know what [bad data quality in information system security documentation] is if I see it."*. However, all stakeholders agreed that if existing information system security documentation contradicts the (newly created) information system security documentation during the IS security and risk management process, special attention should be given to the areas of the information system where contradictions exist.

The observation that, in absence of formal data quality models and structured information system security documentation, contradictions in information system security documentation are viable indicators for potential security problems, is further examined in the confirmatory study by testing the hypothesis:

> **H2:** Contradictions between pre-existing information system security documentation and information system security documentation created by stakeholders as part of an ongoing IS security and risk management are viable indicators for the data quality of information system security documentation and therefore potential security problems.

Finally, the risk manager should be able to select and prioritize areas of the information system for investigation in the information

system security documentation process by some metric in case they need to prioritize due to limited time and budget. We therefore formulated the following hypothesis (cf. [17]):

> **H3:** Prioritization of information system components according to identified contradictions in the comparison of information system security documentation created by stakeholders with pre-existing information system security documentation is viable and improves the quality of early stages of the IS security and risk management process.

5. CONFIRMATORY STUDY

To validate the hypotheses and to further triangulate the results from the exploratory study, four case studies were conducted at the organization under investigation. Four components of the information system under investigation were selected for an in-depth analysis. Stakeholders from the organization (including the stakeholders from the exploratory study) were asked to participate in each of the assessments. Information on the expected results from IS security risk analysis were gathered in close collaboration with senior risk managers.

5.1 Measurement setting

We devised the measurement setting to validate the hypotheses in our confirmatory study. The five step process was executed for each component of the information system under investigation.

- **Step 1 - Collection of information system security documentation:** In this step, we collected any available information system security documentation at the organization under analysis. We worked together with process owners and information system stakeholders to identify any written artifacts.

- **Step 2 - Creation of reference models:** In this step, we "sanitized" any information system security documentation identified in the previous step by converting all documents in a common format and simplifying terminology. We created a information system security documentation reference model from the available documentation. This step required multiple rounds of feedback with stakeholders from the organization to clarify terminology and notations used.

- **Step 3 - Stakeholder interviews and model creation:** In this step, we asked stakeholders to elicit security requirements for the components of the information system under investigation. This required stakeholders to recreate information system security documentation to a large degree. We collected both verbal statements from stakeholders as well as models and artifacts created on paper / whiteboard during multiple workshops.

- **Step 4 - Creation of models for comparison:** In this step, we again "sanitized" the information system security documentation created by stakeholders in the previous step. We created information system security documentation models describing the security aspects of the information system under investigation from the artifacts produced by stakeholders.

- **Step 5 - Identification of contradictions:** In the last step, we compared the models created in step 2 against the models created in step 4 and identified contradictions between them.

For each contradiction identified, a survey was used. The survey items used to measure the research model variables were primarily derived from the qualitative study. All model constructs were measured with indicators are described next.

Contradictions in the asset model: Omitted assets (O_a): we analyzed which assets could be found in the reference models but not in the models created from stakeholder input. New assets (O_n): We analyzed which assets were found in the comparison models, but not in the reference models. And (O_c): we analyzed asset elements that were included in both models, but were described with different attributes.

Contradictions in the security requirements model: Following the taxonomy proposed in [16], we observed inner specification contradictions (S_i), outer specification contradictions (S_o), process contradictions (S_p) and source contradictions (S_s). Contradictions related to roles and risks could not be observed as those were out of scope of this research project. Table 3 includes examples for the previously defined measures.

5.2 Data Collection

Content validity We made an effort to ensure that the modeling tasks were clearly understood by the participants and that the informants responded to questions that we intended to ask. The survey was conducted verbally and clarifications were provided by the researchers. Participants could create models on a whiteboard or paper and were provided with access to any organizational knowledge source that is normally available to them. During the workshops, researchers modeled the artifacts described by stakeholder live in Archimate [5] for further clarification and to avoid inconsistencies due to different notations used by different stakeholders.

Survey study We conducted each workshop of the study at the premises of the organization under investigation and told stakeholders to view the researchers as risk managers conducting an IS security risk analysis. To perform steps 1 and 2, we contacted selected stakeholders from the organization responsible for the management of the internal knowledge base and documentation system to obtain access to relevant information system security documentation. The reference models (Step 2) were created by researchers. To perform steps 3 and 4 with all stakeholders, we went through all components of the information system while asking the survey questions and voice recording their answers. All stakeholders were promised anonymity and the organization was promised confidentiality regarding specific security risk related results and the architecture of the IS under investigation.

We interviewed the stakeholders for at least one hour per workshop. All participants were IS professionals and were product manager or senior developers. Despite the small sample size, we are confident that we provide a reasonably adequate representation of the target population, as we are not interested in perceived effects (requiring a broad sample size) but rather objectively measurable influence in IS security risk management, which would not be gatherable in a broad fashion. A discussion of further limitations and future evaluation in a broader study is presented in the next section.

As the exploratory study has shown, it was hard to define proper quality metrics to assess and evaluate the data quality of information system security documentation. Therefore, and to test hypothesis H2, we compared the number of security requirements for a specific components that were elicited a) without utilization of the identified contradictions and b) with utilization of the identified contradictions. For both settings, a workshop was held at the organization and the participating stakeholders were different (except for one CISO who attended both meetings).

5.3 Analysis

The descriptive statistics of the data are provided in Table 1 and Table 2. Each line contains the respective measurements for each IS Artifact under investigation that was in the scope of this study. The column "entire IS" aggregates the findings of all artifacts that are part of the overall IS. The number of security requirements elicited (SR_{wm}) is shown in the last row. The number of total elicited security requirements is smaller (marked with *) than the sum of each single security requirement, as some security requirements apply to multiple IS artifacts.

We found that outdated documentation (On) explained better than assets that were omitted by stakeholders (Oa) the contribution to the number of elicited security requirements, indicating that outdated information system security documentation is a major inhibitor to IS security and risk management processes. Stakeholders also agreed during the first exploratory study that outdated information system security documentation is an indicator for potential security issues. The more information system components were found that were not documented, the more security requirements were elicited Both observations seem to confirm H1.

The results of the two workshops that were held to validate hypothesis H2 (Are contradictions in information system security documentation a viable indicator for data quality and underlying security issues?) had shown that the number of security requirements that were elicited increased if stakeholders focused on the identified contradictions. We found that using our proposed contradictions method in information system security documentation vastly improved the number of elicited security requirements SR_{wm} as compared to the number of elicited security requirements SR_{wo} that were elicited without our method (9 vs 4 and 11 vs 3).

	IS Artifact 1	IS Artifact 2
O_a	2	3
O_n	3	5
O_c	2	1
S_i	1	8
S_o	3	0
S_P	0	2
S_S	0	0
SR_{wo}	4	3
SR_{wm}	9	6

Table 2: Results from eliciting security requirements for two information system artifacts with (SR_{wm}) and without (SR_{wo}) information system security documentation contradictions.

To analyze the resulting security requirements in terms of quantity and quality, we validated whether the elicited security requirements a) had an understandable description, b) were linked to at least one artifact of the IS, and c) were linked to at least one business source (e.g. customer contract, law) that establishes the business need for each security requirement. If all three conditions were met, we counted the security requirement as properly elicited. Then (depending on the context) those security requirements were matched to the set of already elicited security requirements from a previous IS security risk analysis (i.e. without our information system security documentation contradiction approach).

As a result, we could confirm the hypothesized relationship between existing contradictions in information system security documentation and their possible contribution to the IS security risk management process. Furthermore, we could confirm the hypothesized possibility to prioritize and select areas of the information system based identified contradictions in information system security documentation covering these areas in the IS security risk management process. The following section discusses the results in more detail and presents contributions to research and industry.

6. DISCUSSION

The present paper examined data quality of existing information system security documentation through contradictions identified in the comparison with information system security documentation created during an ongoing IS security and risk management process. In a multi-method research study we assessed the impact of identified contradictions on the IS security and risk management process. Utilization of contradictions to structure and prioritize areas of the IS for investigation was shown to improve the elicited security requirements in both number and accuracy. Thus, our proposed method of indirectly assessing data quality of information system security documentation through contradictions was found to add value to an organization's IS security and risk management process. We observed that outdated information system security documentation was the most important predictor for potential security issues.

6.1 Research Contribution

In extension to existing research on user participation and experimentation in IS security and risk management, the present study examined how data quality of information system security documentation impacts the IS security and risk management. Both the qualitative and quantitative studies found evidence that the data quality of information system security documentation, correlates with potential security risks and that contradictions of information system security documentation created by stakeholders and existing information system security documentation is a viable measure to support the IS security and risk management process. This study provides a first step towards the analysis of data quality of information system security documentation and its contribution to the IS security and risk management process. Secondly, the multi-method research design of the study contributed a first method of identifying data quality issues in information system security documentation within an ongoing IS security and risk management process.

6.2 Implications for Practice

The results of the present study at first and foremost add to the growing body of evidence that suggest that documentation of IS and its security are, together with stakeholder contribution the most important success factors of IS security and risk management. As our research has shown, it is highly desirable for organizations to not only document the security of their IS once, but to keep it continuously updated. Also, identified gaps in information system security documentation should not only be seen as an opportunity to update the information system security documentation but also to investigate potential security issues in the IS covered by that document.

A second implication of the study is the call for increased transparency of IS security documentation and the need for standardized information system security documentation formats. Study findings suggest that there is a benefit from making information system security documentation available to all stakeholders. In particular, it seems to be desirable to include a thorough analysis of existing information system security documentation in the ongoing IS security and risk management process to maximize results.

Finally, study findings suggest that the utilization of identified contradictions in the IS security and risk management process is highly desirable and that the proposed method can lead to a better fit of IS security risk analysis results to the business needs.

	IS Artifact 1	IS artifact 2	IS artifact 3	IS artifact 4	IS artifact 5	Entire IS
O_a	2	3	7	0	4	16
O_n	3	5	0	2	1	11
O_c	2	1	1	0	3	7
S_i	1	8	0	1	1	11
S_o	3	0	2	0	0	5
S_P	0	2	0	1	0	3
S_S	0	0	2	0	0	2
SR_{wm}	9	6	11	1	5	21*

Table 1: Measurement results for the IS artifacts under investigation.

O_a	The stakeholders did not identify components that were documented. *Reference:* All existing components are A-Z *Comparison:* All existing components are A-F
O_n	The information system security documentation was outdated and did not include a component mentioned by the stakeholders. *Reference:* All existing components are A-F *Comparison:* All existing components are A-Z
O_c	Description of assets contained contradictions *Reference:* Components A and B run on VM01 on Cluster01 *Comparison:* Component A runs on VM01 and B runs on VM02 on Cluster01
S_i	The description of the security requirements differs in content. *Reference:* Security Requirement 001: "[...] All ports must be blocked for incoming traffic" *Comparison:* Security Requirement 001: "[...] No incoming traffic must be accepted."
S_o	The security requirement is linked to a different asset. *Reference:* Security Requirement 001 applies to components A,B,C *Comparison:* Security Requirement 001 applies to components A,B,F
S_p	A security related process was described differently *Reference:* Stakeholder A is responsible for the secure data removal process *Comparison:* Stakeholder B is responsible for the secure data removal process
S_s	A security requirements source was differently described *Reference:* Law XYZ applies to components A,B,C *Comparison:* Law XYZ applies to components A,C

Table 3: Observed instances of identified contradictions.

6.3 Study Limitations

Several limitations of this study need to be acknowledged. First, contradictions in the information system security documentation were selected for inclusion based on a simple yes/no scheme. This measurement might contain subjective errors and should therefore be used with caution.

A second limitation of the study is that it was conducted within the relatively low population of two organizations. This limitation is applicable to all surveys with an in-depth focus on a problem from industry, where objective experimentation or broad surveys are not possible. To limit the threat to generalizability of the findings, we tried to exclude industry-specific security requirements for measurement and made sure that the IS security and risk management analysis process did not require industry-specific knowledge.

A third limitation of the present study stems from the fact that contradictions were identified in models created by the researchers, based on the input documents received from the organizations. Due to organizational constraints at the organizations under investigation, it was not possible to conduct group modeling sessions with multiple rounds of feedback. In particular, step 2 was created without any feedback from the organization (apart from some clarifications) and thus might introduce subjective errors. We tried to mitigate these issues by including any organizational knowledge source available to gather information.

A fourth limitation results from the modeling process itself. As we used ArchiMate for modeling during the workshops and to create our reference models, errors might have been introduced as not all stakeholders were familiar with the tool and notation. We tried to mitigate this issue by explaining the notation and provided clarification if stakeholders had problems with it.

6.4 Suggestions for Future Research

The present study suggests two areas where future research would be valuable. First, a broad examination of information system security documentation and the value it provides to organizations is required. The present study examined information system security documentation from a rather abstract point of view. Specific aspects of the information system security documentation and associated processes might be worthwhile to investigate in future studies, including different workflows and tools currently used by industry and data management strategies.

Given, that information system security documentation data quality was found to be an important indicator for possible security issues, it seems worthwhile to investigate the alignment of business needs, IS security risks and documentation further. For example, how can data quality and improvements be valuated? Are existing processes to manage information system security documentation sufficient? Which automated tools can be utilized to continuously update and adapt information system security documentation?

7. CONCLUSIONS

The present study provides evidence that data quality of information system security documentation is a major contributor to information system security documentation processes and that an approach based on identified contradictions in information system security documentation is a viable measurement. Identified contradictions in information system security documentation contributed to identified security requirements and uncovered potential security issues.

IS security risk managers can utilize the method proposed in the present study to prioritize the analysis of different information system components in the IS security and risk management process using an objective process.

8. ACKNOWLEDGMENTS

This work was supported by the Austrian Federal Ministry of Economy (BMWFW), QE LaB - Living Models for Open Systems (FFG 822740) and the Tyrolean business development agency through the Stiftungsassistenz QE-Lab.

9. REFERENCES

[1] R. Alavi, S. Islam, and H. Mouratidis. A conceptual framework to analyze human factors of information security management system (isms) in organizations. In T. Tryfonas and I. Askoxylakis, editors, *Human Aspects of Information Security, Privacy, and Trust*, volume 8533 of *Lecture Notes in Computer Science*, pages 297–305. Springer International Publishing, 2014.

[2] I. Benbasat. An Empirical Study of Rationality-Based Beliefs in Information Systems Security. *MIS Quarterly*, 34(3):523–548, 2010.

[3] Computer Security Institute. CSI Computer Crime & Security Survey. Technical report, Computer Security Institute, 2008.

[4] Ernst and Young. Into the cloud, out of the fog; Global Information Security Survey. Technical Report November, Yourg, Ernst, 2011.

[5] T. O. Group. *{ArchiMate} 1.0 Specification*. Van Haren Series. Van Haren Publishing, 2009.

[6] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly. Understanding nonmalicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems*, 28(2):203–236, 2011.

[7] R. L. Heath and H. D. O'Hair. *Handbook of risk and crisis communication*. Routledge, 2010.

[8] F. Kohlbacher. The use of qualitative content analysis in case study research. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 7(1), 2006.

[9] E. A. Locke, M. Alavi, and J. A. Wagner III. Participation in decision making: An information exchange perspective. In *Research in personnel and human resources management, Vol. 15*, pages 293–331. Elsevier Science/JAI Press, US, 1997.

[10] M. L. Markus and J.-Y. Mao. Participation in development and implementation-updating an old, tired concept for today's IS contexts. *Journal of the Association for Information Systems*, 5(11):14, 2004.

[11] R. Mejias. An integrative model of information security awareness for assessing information systems security risk. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 3258–3267, Jan 2012.

[12] T. R. Peltier. *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Taylor & Francis Ltd, Hoboken, NJ, 2013.

[13] P. Puhakainen and M. Siponen. Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly*, 34(4):757–778, 2010.

[14] J. J. Ryan, T. a. Mazzuchi, D. J. Ryan, J. Lopez de la Cruz, and R. Cooke. Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research*, 39(4):774–784, Apr. 2012.

[15] M. K. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren. Action design research. *MIS Quarterly*, 35(1):37–56, Mar. 2011.

[16] C. Sillaber and R. Breu. Quality matters: Systematizing quality deficiencies in the documentation of business security requirements. In *Availability, Reliability and Security (ARES), 2014 Ninth International Conference on*, pages 251–258, September 2014.

[17] C. Sillaber and R. Breu. Using business process model awareness to improve stakeholder participation in information systems security risk management processes. In *Wirtschaftsinformatik Proceedings*, 2015. Paper 79.

[18] M. Siponen and H. Oinas-Kukkonen. A review of information security issues and respective research contributions. *ACM Sigmis Database*, 38(1):60–80, 2007.

[19] M. T. Siponen. Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management & Computer Security*, 8(5):197–209, 2000.

[20] J. L. Spears and H. Barki. User participation in information systems security risk management. *MIS quarterly*, 34(3):503–522, 2010.

[21] J. Stanton, K. Stam, P. Mastrangelo, and J. Jolton. Behavioral Information Security. *Human-Computer Interaction and Management Information Systems: Foundations*, page 262, 2006.

[22] P. J. Steinbart, R. L. Raschke, G. Gal, and W. N. Dilla. The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems*, 13(3):228 – 243, 2012. 2011 Research Symposium on Information Integrity and Information Systems Assurance.

[23] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1):1–11, Jan. 2011.

[24] H. Susanto, M. N. Almunawar, and Y. C. Tuan. Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences*, 11(5):2011, 2011.

[25] A. Vance. Neutralizaiton: New Insights into the Problem of Employee Information Systems Security. *MIS Quarterly*, 34(3):487–502, 2010.

[26] V. Verendel. Quantified security is a weak hypothesis. *Proceedings of the 2009 workshop on New security paradigms workshop - NSPW '09*, page 37, 2009.

[27] J. Wade. The weak link in IT security. *Risk Management*, 51(7):32–37, 2004.