Ontology-based information security compliance determination and control selection on the example of ISO 27002

Stefan Fenz and Thomas Neubauer
SBA Research and Vienna University of Technology, Vienna, Austria

Received 13 February 2018
Revised 9 April 2018
28 May 2018
Accepted 28 May 2018

Abstract

Purpose – The purpose of this paper is to provide a method to formalize information security control descriptions and a decision support system increasing the automation level and, therefore, the cost efficiency of the information security compliance checking process. The authors advanced the state-of-the-art by developing and applying the method to ISO 27002 information security controls and by developing a semantic decision support system.

Design/methodology/approach – The research has been conducted under design science principles. The formalized information security controls were used in a compliance/risk management decision support system which has been evaluated with experts and end-users in real-world environments.

Findings – There are different ways of obtaining compliance to information security standards. For example, by implementing countermeasures of different quality depending on the protection needs of the organization. The authors developed decision support mechanisms which use the formal control descriptions as input to support the decision-maker at identifying the most appropriate countermeasure strategy based on cost and risk reduction potential.

Originality/value – Formalizing and mapping the ISO 27002 controls to the security ontology enabled the authors to automatically determine the compliance status and organization-wide risk-level based on the formal control descriptions and the modelled environment, including organizational structures, IT infrastructure, available countermeasures, etc. Furthermore, it allowed them to automatically determine which countermeasures are missing to ensure compliance and to decrease the risk to an acceptable level.

Keywords Decision support systems, Compliance, Organizations, Risk management, security, Ontology

Paper type Research paper

Introduction

Cyber incidents are one of the top emerging risks in companies for the long-term future. Accenture and Ponemon Insitute (2017) state that the annualized cost of cyber security in 2017 to US$11.7mn on average per company (basis: 254 companies that have been analyzed in the study). The costs for cyber security increase by 22.7 per cent per year. The number of

This research was funded by the FFG – Austrian Research Promotion Agency (COMET K1 center SBA Research) and the WWTF – Vienna Science and Technology Fund (project FORISK).

Information & Computer Security
Vol. 26 No. 5, 2018
pp. 551-567
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-02-2018-0020

security breaches increases by 27.4 per cent per year. With more companies connecting to the internet, for example, because of the rise of the Internet of Things, the cost of cyber-crime will continue to increase rapidly. Apart from the financial costs attacked companies have to deal with damages to reputation, competitiveness and innovation.

Therefore, companies need approaches to systematically gather and structure data on cyber-crime to make better decisions about risk and policy (OECD, 2012). Industry standards, such as the ISO 27000 series, support companies in this matter and require evaluating the information security management system and the associated security measures on a continuous basis. Effective risk management has to consider recent changes in the (internal) infrastructure and the (external) environment and inform the decision-maker about upcoming threats and required changes to the countermeasures (Dobie, 2016). Traditional information security risk management software products support companies at these tasks, but provide a limited degree of automation at mapping the information security domain knowledge on the concrete situation of the company. Ontology-based risk management approaches use semantic knowledge bases and reasoning engines to automatically derive the compliance status based on inventory data about the company assets and already implemented countermeasures. The main advantage of ontology-based approach is that the user only has to inventory the company assets and countermeasures, reasoning engines decide automatically which controls are fulfilled and how much this affects the compliance level of the company. A further advantage is that the underlying ontology is encoded in a standardized markup language (W3C OWL) and can be easily extended and integrated in compliance and risk management software solutions.

Security ontologies have been developed in the past 15 years for a broad range of application fields:

- reusable knowledge in security requirements engineering (Souag *et al.*, 2015);
- high-level ontologies about information security (Schumacher, 2003; Avizienis *et al.*, 2004; Kim *et al.*, 2005; Herzog *et al.*, 2007);
- security incident classification (Martimiano and dos Santos Moreira, 2005);
- secure software development (Karyda *et al.*, 2006);
- system security-level assessment (Solic *et al.*, 2015);
- semantic security policy matching (Di Modica and Tomarchio, 2016); and
- web application attack prediction (Salini and Shenbagam, 2015).

The method described in this paper updates the currently largest publicly available IT security ontology (Fenz and Ekelhart, 2009) by formal control descriptions of the ISO 27002 standard. The ontology was chosen as the basis for this work because it is already productively used in risk management software solutions and provides the necessary knowledge structure to embed a formal representation of the ISO 27002 standard. Formalizing and integrating the ISO 27002 controls in the security ontology enables the developed semantic decision support system to automatically determine the organization-wide compliance status. This information can be used to automatically determine which missing countermeasures are required to be compliant to ISO 27001[1]. Consequently, the decision-maker is informed about the measures required to decrease the risk to an acceptable level.

Related work and research need

Existing approaches in the field of information security compliance and risk management require the user to run through the following phases (Fenz *et al.*, 2014):

- systematic inventory of assets, their acceptable risk levels and already implemented countermeasures;
- assessment of potential threats and vulnerabilities;
- risk determination by combing threat probability and impact in the context of each asset;
- identification of controls which can be used to reduce the risk to an acceptable level; and
- evaluation of potential controls with regard to their cost/benefit ratio and subsequent implementation of the controls.

Fenz *et al.* (2014) identified common challenges when implementing information security risk management approaches at companies to be in the areas of asset and countermeasure inventory identification, asset value assignment, risk prediction, lack of understanding and the overconfidence effect, knowledge sharing and risk versus cost trade-offs.

These challenges stem from the fact that the information security domain is a fast-moving and ever-changing field. The company assets which should be protected can change on a daily basis. For example the importance of certain assets rises over time because of their changing involvement in business critical processes. In addition, new threats emerge and new vulnerabilities have to be mitigated by new countermeasures. This fast-moving field makes it difficult for traditional risk and compliance management tools to reflect the most recent risk and compliance level and to provide appropriate countermeasures to the decision maker.

The hypothesis of this work is that the degree of automation within the necessary knowledge processing and control identification has to be increased to ensure that recent developments are taken into account.

While semantic information security knowledge bases which can be used to automate the knowledge processing are available, a research need was identified regarding:

- methods to extend these knowledge bases with formal information security control descriptions; and
- decision support systems that are based on semantic knowledge bases and provide specific control implementation guidance to the decision-maker.

Research method and theoretical background

This research has been conducted on the basis of design science principles. Design science aims at creating new and innovative artifacts to extend the boundaries of human and organizational capabilities (Hevner *et al.*, 2004). The *design artifact* of this work is an ontology-based decision support system for automated information security control compliance determination and control selection. The *relevance of the problem* is based on the strong need of organizations to conduct risk and compliance management activities in an efficient and comprehensive way. The design artifact has been created by an iterative search and evaluation process. The *evaluation* of the research results has been conducted by expert evaluations and real-world deployments in the context of ISO 27002 controls. End-users were involved in the design and evaluation process to ensure the applicability of the research results.

The adequacy of the research is justified by applying the following theoretical background:

- *Normative decision theory*: the decision-maker acts rationally and has to be informed about the costs, benefits and consequences of the decision within the given environment.

- *Stakeholder theory*: decisions involve and affect various stakeholders, that is, a decision support system has to translate the technical knowledge to the decision dimensions, such as financial or political figures, to support stakeholders in identifying the best decision option.

In the following sections, we describe the knowledge base, the developed method to formalize information security controls and the decision support system which has been developed to validate the results in consultation with experts and end-users.

The knowledge base

A decision support system for automatically determining ISO 27001 compliance and identifying missing control implementations requires a machine-readable knowledge base regarding:

- the ISO 27002 controls;
- their relation to concrete control implementations (i.e. concrete information security products); and
- the concrete application environment (i.e. knowledge about the organization being certified against ISO 27001).

This knowledge base needs not only to be machine-readable, but also has to allow reasoning engines to interpret the existing knowledge to derive new knowledge. For example: interpreting a formal ISO 27002 control description, checking the corresponding concrete implementation at the organization and automatically deriving the compliance status regarding this control.

Ontology languages, such as the W3C Web Ontology Language (OWL), can be used to formally describe a knowledge domain. OWL has a rich expressiveness and allows us to model concepts, their relations and their domain-specific characteristics on a highly granular level. Reasoners can be used together with OWL ontologies to derive new facts from the existing knowledge body.

Our related work review has shown that the security ontology by Fenz *et al.* (2011) can be efficiently extended by ISO 27002 control descriptions and is, therefore, suited as knowledge base for the developed security control formalization method and the final decision support system of this research. The ontology is currently the largest publicly available security ontology. It is already used in industry products and Fenz *et al.* (2016) illustrate how this knowledge base can be used for compliance checking. The proposed approach for extending the knowledge base by integrating the ISO 27002 control descriptions is illustrated in Figure 1.

It is based on the security ontology described in Fenz and Ekelhart (2009) and on previous work on mapping the ISO 27001 standard to the security ontology (Neubauer *et al.*, 2008):

- The mapping methodology shown on the top of Figure 1 is used to transform the informal ISO 27002 knowledge into a formal and machine-readable form. First, the ontology in which the knowledge will be mapped is analyzed for existing concepts and relations. Second, the ISO 27002 controls are analyzed for domain-relevant concepts and relations. Based on the results of Steps 1 and 2, the main concepts and relations are mapped to the ontology. In the last step, the formal control implementation descriptions are created within the ontology based on the informal descriptions of the ISO 27002 standard.

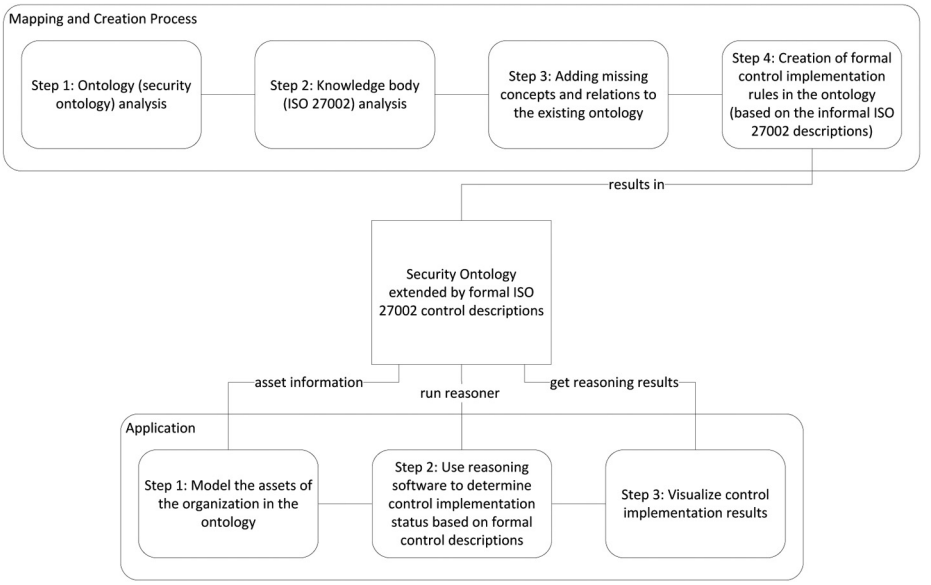

Figure 1.
Creation process of the knowledge base

- After the mapping, the knowledge base (ontology) consists of a formal representation of the ISO 27002 controls, their relations to the ISO 27001 control groups and objectives, and a formal representation of the control implementation rules.
- In the application phase, we demonstrate how the research results can be used in a real-world setting. Supported by a tool, the organization models its assets within the ontological structure. By interpreting the formal control descriptions and the modeled assets, a reasoner (software which infers logical consequences from a set of asserted facts) classifies all assets which fulfill one or more of the ISO 27002 controls as compliant assets. A software tool visualizes the results and provides immediate feedback regarding the compliance level of the organization.

Example: The ISO 27002 standard states that data backup procedures have to be in place. Within the security ontology, this fact is modeled by a formal control description which requires that each organization which is modeled within the ontology has to be linked with some (at least one) instance of a data backup policy concept (Figure 2). In the application phase, a reasoning software will process this formal control description and automatically determine if it is fulfilled or not. If the organization has a data backup policy in place, then it was modeled within the ontology in Step 1 of the application phase (Figure 1) and the reasoner classifies the entire organization as compliant to this specific data backup control. Figure 2 shows how this example is modeled in the security ontology. The concept "Data Backup Control Compliant Organization" specifies that organizations which implement a data backup policy are compliant to this control. The relation "control_compliantWith_Control" specifies that compliance to this control is required to be compliant to ISO 27002 control "A.10.5.1 Information back-up". Figure 2 shows that the data backup control is linked to other standard controls and is, therefore, used in more than one certification context.

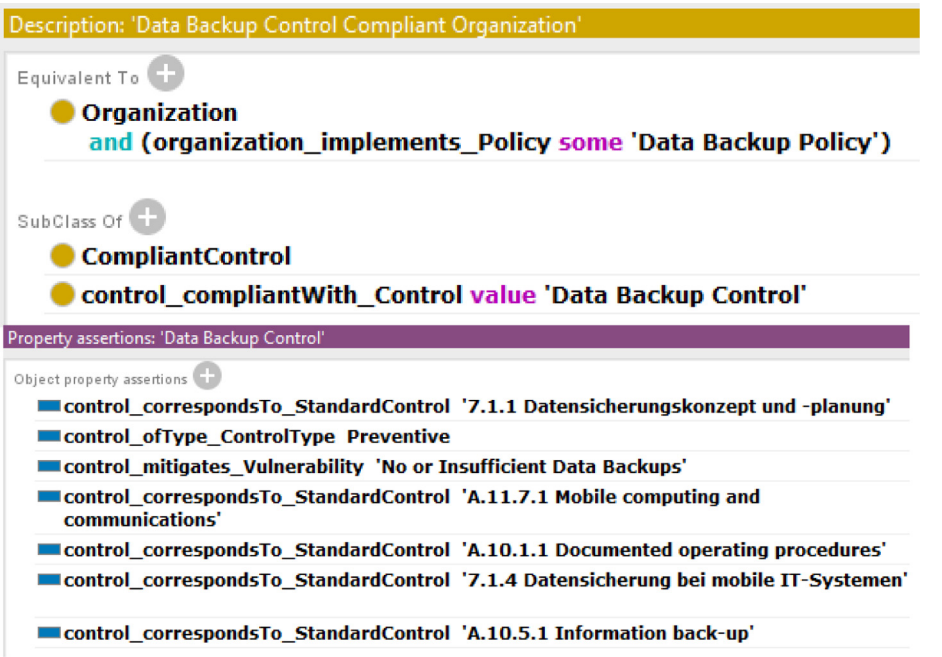

Figure 2.
Data backup control

The usage of ontologies has many advantages over simple spreadsheets or relational databases. The main advantages are without doubt their interoperability and the possibility to analyze the stored facts by software-based semantic reasoners. Furthermore, because of their flexible structure, new entities and relations can be implemented without drawbacks, as the definitions can be implemented on-top and incrementally. The overall purpose of our work was to enrich the security ontology with formal rules derived from the ISO 27002 standard (ISO/IEC 27002, 2013) to ease the compliance checking by enabling organizations to query, visualize and analyze the knowledge base.

For the compliance check, an organization's assets are mapped in the knowledge base and serve as snapshot of the organization's current security state that is considered in the reasoning process. The formalized controls and the snapshot are then evaluated by a reasoner, which infers the compliance status of the organization's implemented controls with the controls defined in the ISO 27002. Regardless of the inferred results, the implemented knowledge base and the inferred knowledge of the reasoner can be queried, visualized and analyzed. Because of the flexible ontological characteristics, extensions could be incrementally implemented and various mitigation strategies can be implemented in short time, leading to a sophisticated simulation system of security threats. A single change to an organization's security configuration can affect its compliance with many security controls. This leads to the need for huge effort in the auditing and analysis of the organization's security measures. However, the proposed framework will give organizations a simpler way to implement such changes by enabling them to model their entire infrastructure and find appropriate mitigation strategies based on the reasoner's findings.

Inventory and decision support

To validate the developed method and the resulting security ontology including the formal ISO 27002 control descriptions, we developed a compliance and risk management decision support system which is capable of using the security ontology as the underlying knowledge base. Developing this prototype was necessary to validate the research results with expert- and end-users. The very technical ontology and reasoner output could only be used in lab experiments but not in real-world environments which also involve end-users. In this section, we briefly describe the prototype which has been used in the validation phase of our research.

The prototype integrates the security ontology reflecting the modelled asset classes, threats, formal control descriptions and the compliance/risk calculation based on the relations modelled in the security ontology. The implementation is a web application that consistently combines the methodologies to assist the whole process of compliance and risk evaluation. In the last step, it also provides suggestions on how the overall risk can be efficiently reduced.

The asset inventory (Figures 3 and 4) allows the user to define the company assets in a hierarchical way, in which the child assets are meant to be physically located within the parent asset. The user needs to assign an ontology class to the added asset, which indicates its specific type, like Building, Workstation, etc.

Based on the formal ISO 27002 controls, the countermeasure inventory allows the user to select the security policies that his company already implements, as well as the countermeasures implemented on individual assets. The information which policies should be implemented on the company level is provided by the ontology to the tool. Furthermore, the ontology defines a priori which countermeasure classes are relevant for which asset classes and should be implemented in the context of ISO 27002. The user indicates in the inventory phase which *concrete* countermeasure implementations are present at the *individual* assets and which *concrete* policies are implemented in the company. Example: the ontology defines that a cooling system should be implemented in server rooms; based on that, the user has to select in the inventory phase the concrete

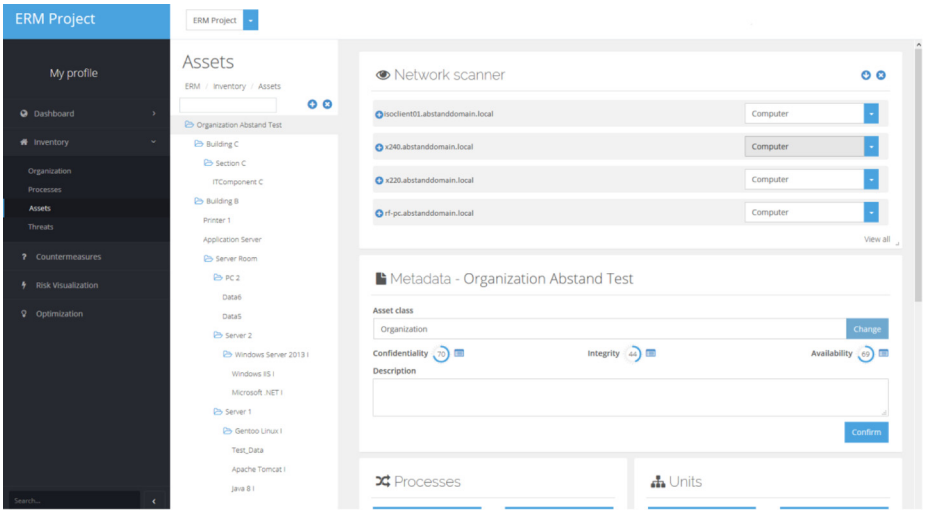

Figure 3.
Asset inventory process

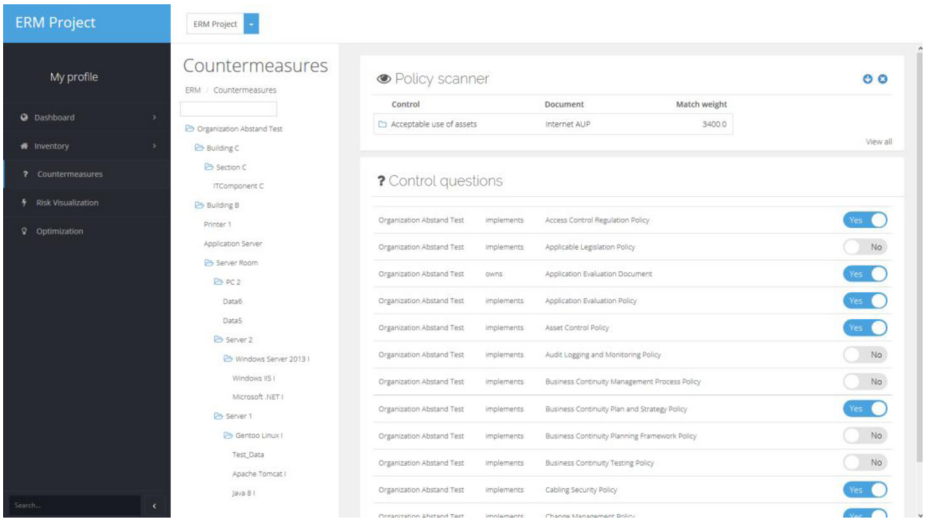

Figure 4.
Policy inventory process

cooling system type which is implemented in the specific server room. The cooling system type and its effectiveness and costs attributes are provided by the ontology to the tool.

The risk visualization builds upon the knowledge model of the underlying security ontology which formally encodes the relationships between threats, vulnerabilities, controls and company assets. Please see Fenz and Ekelhart (2009) for a detailed description of the security ontology. Figure 5 shows how the risk of a certain asset (in this case the server room) is visualized. The overall risk figure given the current setting of the server room is 31. The 31 is the product of the integrity risk of 49, the availability risk of 9, the integrity weight of 54 per cent and the availability weight of 46 per cent ($49 \times 0.54 + 9 \times 0.46 = 30.6$). The integrity and availability weights are chosen by the user in the setup phase and have to sum up to 1. The integrity and availability risks are the product of the impact and the threat probability values. For the integrity of the server room, it is $74 \times 0{,}66 = 48.84$, for the availability of the server room it is $21 \times 0.43 = 9.03$. The integrity and availability impact values are derived from the inventory phase, in which the user has to answer a set of questions regarding the importance of each asset for the company (Cervantes *et al.*, 2014) for further details on the questionnaire approach). The threat probabilities are assessed by checking how much already implemented countermeasures decrease the occurrence probability of relevant threats (residual probability). The weakest link theorem requires us to select the highest residual probability of each category for our risk calculations. In Figure 5, this would be 66 per cent for the inadmissible temperature and humidity threat (integrity) and 43 per cent for the theft threat (availability).

The threat catalogues of the security ontology distinguish between top- and low-level threats. A top-level threat such as asset damage and asset loss relate directly to a security attribute (integrity and availability) and are connected to several predecessor threats, that is, low-level threats which enable the top-level threat and determine its occurrence probability. Based on already implemented countermeasures, Figure 5 shows the residual occurrence probability for each of these threats.

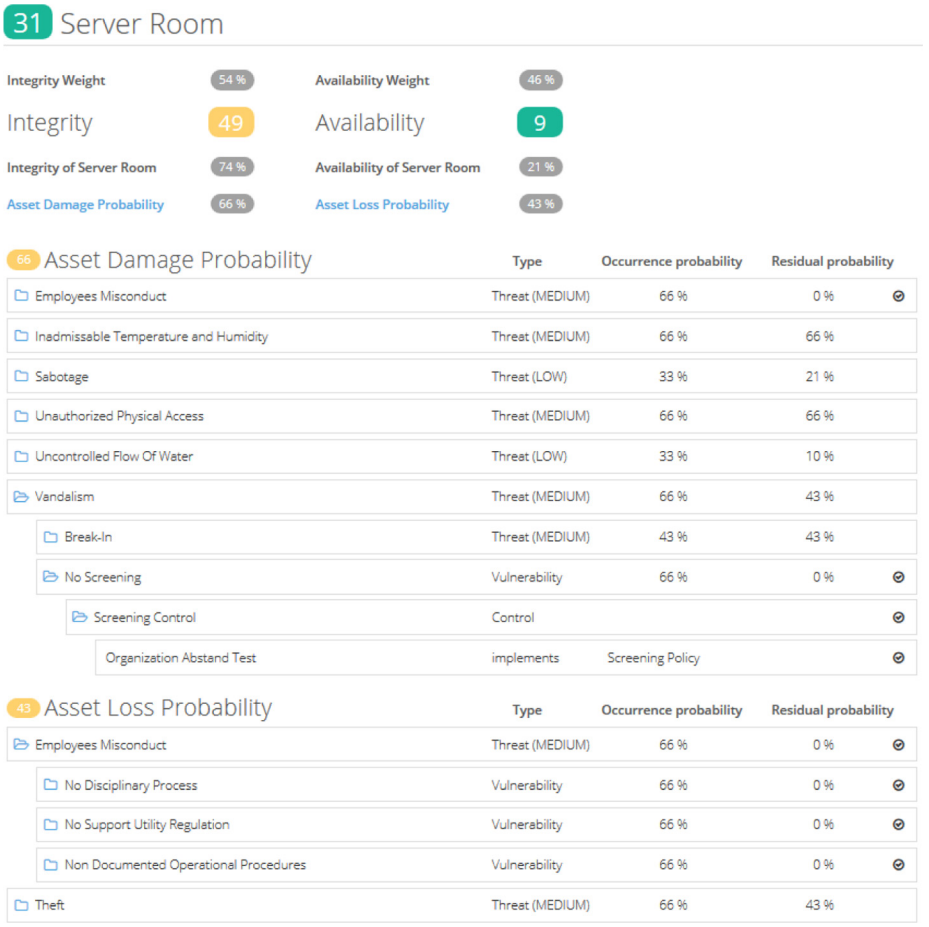

Figure 5.
Occurrence probabilities of the impact-related threats

The threats are presented in a hierarchical structure (Figure 5), where the threat children represent the vulnerabilities that can be exploited by the threat, as well as other threats that can give rise to the threat. Each vulnerability relates to a list of controls, which are required to mitigate it. The connection between vulnerabilities, ISO 27002 controls and their concrete implementation requirements are defined in the security ontology and were derived from best-practice guidelines, information security standards and other relevant sources. See Section "The Knowledge Base" for a detailed description how the ISO 27002 controls were incorporated into the security ontology.

Whether a standard control is fulfilled by the implemented control measures, or not, is determined by semantic reasoning engines and the formal information security control descriptions. To reduce the threat occurrence probability, it is necessary to cover all of the vulnerabilities it can exploit by implementing the control measures that fulfil the related standard controls.

The optimization user interface provides suggestions on how the overall company risk can be efficiently reduced (Figure 6).

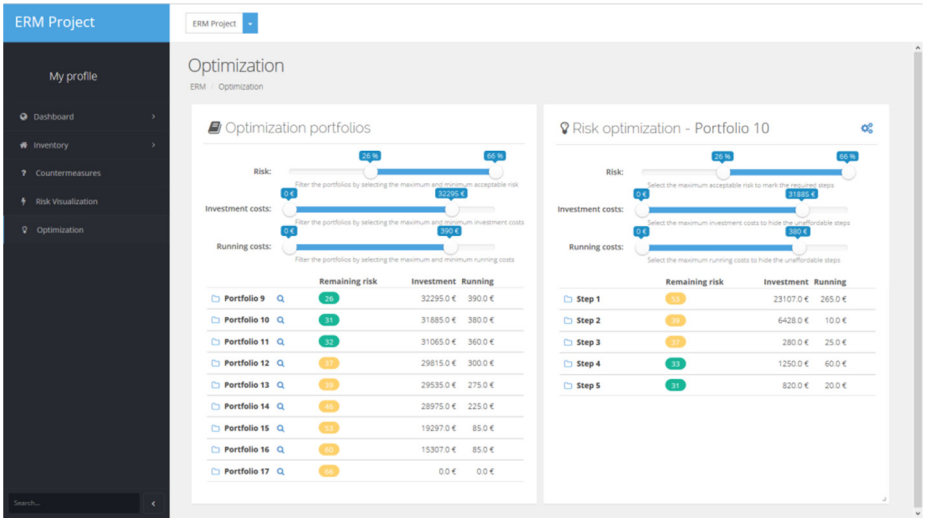

Figure 6.
Countermeasures optimization process

The system presents a list of optimization portfolios for various target risk values. These portfolios are the result of genetic optimization algorithm runs conducted by the tool. The ontology provides the countermeasure gold standard (i.e. implementation of all potential countermeasures to reduce the residual threat probabilities to a minimum) and the currently implemented countermeasures to the optimization component which builds with the help of genetic algorithms countermeasure portfolios which can be used to decrease the overall risk level.

Each portfolio optimizes the investment costs and the running costs required to achieve the acceptable remaining risk. The costs are derived from the security ontology which stores for each countermeasure investment and running cost attributes. In the inventory phase, the user can review these costs and can adapt them to the individual setting if necessary. There can be potentially multiple portfolios for the same acceptable risk value if some portfolios require smaller investment costs, while other portfolios require less running costs. The portfolios consist of sequential optimization steps that lead to a reduction of the overall company risk. The user can adjust the lower and the upper bounds of the acceptable risk, the investment costs, and the running costs, using slider controls. When adjusting the bounds, the displayed portfolios are dynamically filtered to meet the requirements.

Moreover, the maximum acceptable risk influences the minimum investment and running costs, just like the maximum investment and running costs influence the minimum acceptable risk. To reflect these relations, the bounds on the sliders are continually adjusted depending on what values the displayed portfolios provide.

The risk optimization widget (Figure 7) displays the optimization steps of the selected optimization portfolio based on the output of the genetic algorithm. The steps are supposed to be implemented in the same order, in which they are presented. Each step is described by its investment costs, running costs and the overall risk value remaining after the completion of the step.

The step is described by a list of required missing control measures that are presented on white rows with their investment costs and running costs (e.g. identification software on

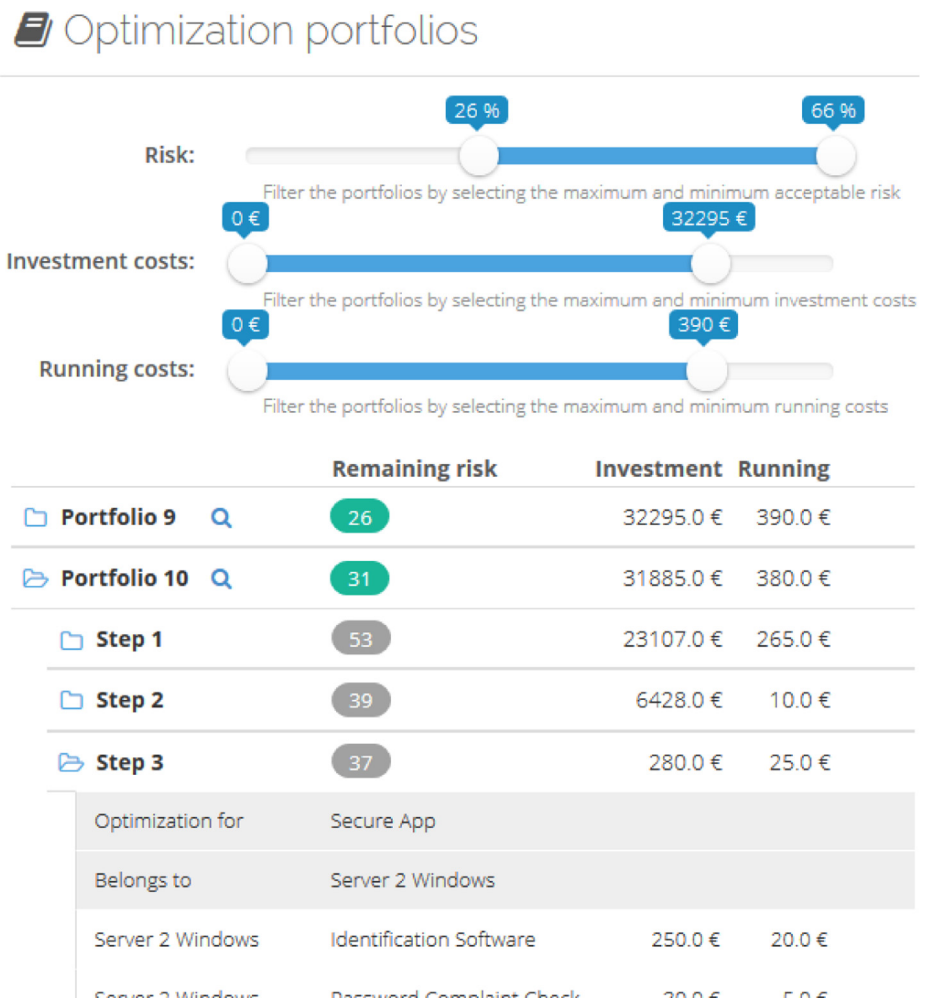

Figure 7.
Interactive decision support

"Server 2 Windows" as shown in Figure 7). The selection of control measures is based on the assets with the highest residual risk level and their physical location. A brief explanation of this selection is provided by rows presented in grey. While the risk optimization in Figure 7 was done for the asset "Secure App", the control has to be implemented on "Server 2 Windows" as it constitutes the host system of "Secure App". To reach risk level of 37 at Portfolio 10/Step 3 for "Secure App" (Figure 7), it is required to implement identification software and password compliant checks on "Server 2 Windows".

The user can again adjust the optimization goals using slider controls. Changing the maximum investment costs and running costs might hide some unaffordable steps. Moreover, changing the maximum acceptable risk might mark some steps as mandatory. The bounds on the sliders are also continually adjusted to reflect the relations between the acceptable risk and the investment and running costs. The sliders act like filters on the data set of all potential optimization portfolios which were determined by the genetic algorithm.

This means that all portfolios are calculated and loaded at runtime and the user uses the sliders to filter those portfolios which fit his requirements in terms of costs and risk level best.

The measures which are included in the steps of the portfolios are automatically determined by the reasoning engine based on the formal information security control descriptions. The reasoner checks which measures are currently implemented within the organization (according to ISO 27002). By comparing the list of measures which should be implemented and the list of measures which are currently implemented we can derive which measures are missing to fulfill a certain information security standard (e.g. ISO 27002). The data for missing measures, such as cost and effectiveness, are stored in the ontology and provided to the decision support system which then can build appropriate measure portfolios for risk reduction.

Validation

In order to validate the developed methodology and the implemented decision support system in a real world environment, we had selected a middle-sized organization in Austria that specializes on highly secure IT solutions. The organization is renowned for the security of its products and makes effort to keep its systems safe to maintain its reputation. With the perspective of improving the security, the company management allowed us to perform the experiment using our implemented tool in the company environment and supported us with information about the company infrastructure and important business processes. Using the collected information, we were able to model the ongoing risk, identify the most critical assets and determine the weakest links. The duration of the validation phase was two weeks, involved two researchers and five employees of the company. The employees devoted 22 hours in total to the validation of the research results by participating in the following activities: introduction to the tool, inventory interviews, risk and countermeasure identification and feedback discussions.

In the following paragraphs, we describe how we conducted each phase of the risk and compliance management process by using the extended security ontology together with the developed decision support system. It can be assumed that risk and compliance management phases are conducted in a similar way in other organizations.

Inventory

This step is necessary to map the assets and already implemented countermeasures of the company to the security ontology and to enable a reasoner to identify potential compliance gaps and risk reduction measures.

The organization is located in a single building and has several departments, some of them consisting of multiple teams. The company does not track the physical location of its assets, but rather maintains a list of employees along with their associated devices. We made a list of important rooms in the company building and assigned them to the related departments[2]. We also performed a network scan, which not only found a number of PCs, but also many virtual machines. Although the network scan could not reveal the exact location of the found hosts, we were able to find out which persons the hosts belonged to and where they worked. We identified the location of some other devices, like servers, printers, access points, switches and routers. After finishing this step, we modeled a large proportion of the company hardware and virtual hosts. The next step focused on identifying the important services and data. After creating the asset hierarchy structure, we assigned proper assets to the individual activities of the modelled business processes. This allowed us to run the process-based calculations and determine the availability requirement of the

related assets. The last step was to estimate the security attribute requirements of the inventoried assets. Some of the estimations could be done by the associated staff, some could be derived automatically. For the remaining assets, we used our own experience to provide the estimations manually.

After gathering the knowledge about the organization, its physical location, environment, business processes and infrastructure, we identified the policies and individual countermeasures that were already implemented in the organization.

Risk identification and feedback

Using the established test environment, we executed the risk and compliance calculation and presented the results to various persons from different professional areas with the goal to acquire feedback from different points of view. We scheduled meetings with representatives from the area of security consulting, sales management, security analysis and research. The participants possessed diverse knowledge in the area of information security. Some of them were experts in specific domains with the ability to understand the underlying methodologies on a deep level. Others had a broad knowledge with the ability to evaluate the usability in practice and the possible applicability in the business environment. This variety turned out to be beneficial and brought us a broad feedback.

The reactions of the respondents were mostly positive. In particular, they commented on the compliance/risk modelling process, the compliance/risk optimization using portfolios and the overall user interface. Some parts of the application received a mixed feedback, especially regarding the applicability in a real-world environment. Some criticism was addressed towards the inventory process, which, even with the help of the provided tools, would require a significant effort.

During the evaluation process, we addressed the implemented methodologies individually to identify possibly improper approaches or parts that require further improvement. The hierarchy structure used to model the company inventory was rated positively. There was a suggestion to add a concept of virtual containers for mobile devices, where the physical location might be volatile. Some respondents considered the entire approach to be rather complex for standard users and rated the comprehensibility as neutral. Process-based calculations also received a mostly positive feedback. There were suggestions to improve the overview of the assigned assets and to extend the model visualization to display the calculated risks.

The ontology integration received very little feedback. Most of the participants had little knowledge about the concept, what likely made it difficult to compare this approach with other possible solutions. We tried to briefly introduce our respondents to ontologies and how they are related to the application. They appreciated the possibility to dynamically modify the underlying security ontology, but some of them were discouraged by the complexity it might represent for users that are not familiar with the concept.

The compliance and risk calculation was rated as closely approximating the real world and the weakest link approach was considered applicable in practice. All of our respondents reacted positively towards the integration of various security attributes. There was also an opinion that the results calculated for individual security attributes should be treated separately and that their aggregation is unnecessary. However, some of the respondents found it difficult to interpret the percentage representation of the calculated results and suggested integration of monetary values.

The optimization component received a positive overall feedback. The respondents commended the generation of cost-effective portfolios and appreciated the way it was bound to the compliance and risk calculation. The filtering options were also considered useful and

the presented results meaningful. There were suggestions to allow optimization on the level of specific organizational units, or individual security attributes. Some criticism was addressed towards the specification of the implementation costs. Some representatives from areas of security consulting and sales management commented that the implementation costs might depend on the specific company and even vary from asset to asset.

We also received some criticism regarding the complexity of the risk visualization. The ontology-based visualization was considered very detailed, but also difficult to understand without a prior explanation. There were suggestions to provide additional widgets for a more simplistic presentation of the results, like for example diagrams and charts showing the calculated risk values. There were also suggestions to provide additional reporting functionality and export of the results into various formats.

Difference to the currently implemented compliance and risk management approach

Currently, the organization uses a traditional risk and compliance management tool which differs in the following ways from the validated approach:

- With the current approach two persons enter the data into the tool, analyze the output and suggest possible countermeasures to the management. The data are not inventoried in a decentralized way by the responsible persons. As risk and compliance management activities are mainly done by two persons, they are not readily available to the remaining company staff.
- The developed approach requires the inventory of each item only once. As soon as the knowledge fragment is stored in the ontology, the reasoner uses it for all required risk and compliance activities. Example: the user states only once that a fire extinguishing system is present in the server room. The reasoner automatically decides how this affects the compliance and risk level in the context of different information security standards such as ISO 27002.
- The developed approach automatically creates cost-efficient countermeasure portfolios which can be implemented to achieve compliance and reduce the residual risk to a defined level. Currently, this has to be done in a manual way which poses the risk that cost-efficient countermeasure portfolios are overlooked.
- Compared to the current approach, the decision support component of the developed approach enables management to make an informed decision regarding a suitable countermeasure portfolio on the basis of the presented cost and residual risk data.

Advantages/disadvantages compared to other methods/tools

The following advantages were identified compared to existing tools (CRISAM Explorer, Ebios, GSTool) in the field of risk and compliance management:

- Knowledge base and formal control descriptions are not encoded in a proprietary format. As the W3C Web Ontology Language (OWL) is used, the security ontology and the formal control descriptions can be used in combination with existing ontology editors and reasoners.
- Modelling the control descriptions and the assets of the company within the security ontology enables the reasoner to automatically draw conclusions regarding the compliance state of the company. The reasoner automatically applies the ISO 27002 knowledge to the actual environment of the company.

- Besides compliance management, the modelled control and environment data can also be used for risk management activities, such as selecting cost-efficient information security controls.
- The semantic knowledge base and the broad availability of editors enable the efficient extension of the knowledge base by further information security standards.
- Using description logics enabled us to define the control fulfillment requirements on a highly granular level and it was also possible to define alternative implementation possibilities.
- Because the compliance status is evaluated based on concrete company assets and countermeasures, the implemented method and decision support system are capable of providing concrete guidance of how and where to implement additional countermeasures (e.g. place an additional fire extinguisher in Room C.1). This guidance includes also investment cost data.

The following disadvantages were identified. However, they are inherent to other comparable tools in the field of risk and compliance management:

- A full inventory of all relevant company assets is necessary. This requires a substantial initial effort across various departments of the company. Automated inventory tools and decentralized data assessment can be used to lower the required effort. The evaluation has shown that the inventory effort is around 30 per cent higher compared to traditional approaches. This finding was verified in lab experiments in which we measured and compared the inventory time of the developed and traditional approaches.
- The formal specification of ISO 27002 controls needs expert experience and knowledge. However, the specifications have to be updated only when a new standard or countermeasure technology becomes available.

Conclusion

The goal of our work was to provide a method for formalizing information security controls, use this formal description in combination with reasoners to derive new knowledge and integrate these components in a decision support system for risk and compliance management to provide decision-makers with comprehensible and technical sound decision options. In this context, we applied the developed method and extended the currently largest publicly available IT security ontology with formal control descriptions of the ISO 27002 standard. Based on that, we implemented a prototype and evaluated the implemented methods and artifacts together with experts and end-users in a medium-sized company.

The evaluation has shown that the developed approach is feasible and the decision options which were generated based on the formal control descriptions were of benefit to the decision-makers. The biggest advantage was that the semantic knowledge base ensures that all generated decision options are in line with the underlying ISO 27002 standard and take the local characteristics of the company (e.g. already installed countermeasures) into account.

Future work

In further research, we aim to extend the cross-standard capabilities of the method. Information security standards beyond ISO 27002 should be supported which requires a method of how to identify overlaps between the standards and a way to consider this at the knowledge modeling process.

Researching on and implementing a cross-standard method enables us to design and conduct a wider validation study. We plan to obtain the following insights from this study:

- How do other organization types and industry fields benefit from the developed approaches?
- How much inventory effort can be saved by applying the approach in a setting which requires compliance checks against multiple information security standards?
- What are the limits of managing the semantic knowledge base in highly dynamic environments such as software security where new software vulnerabilities are discovered on a daily basis?
- What kind of knowledge management approaches can be used to extend and update the underlying security ontology in a collaborative way across multiple organizations?

Notes

1. In the context of the ISO 27000 series, an organization is certified against ISO 27001. ISO 27002 provides the definitions of the corresponding information security controls.
2. It is necessary to model the physical and virtual location of an asset to support the reasoner at determining if information security controls are fulfilled. For example, if a fire extinguisher system is implemented in the room which locates crucial servers.

References

Accenture and Ponemon Insitute (2017), *Cost of Cyber Crime Study, Insight on the Security Investments That Make a Difference*, Accenture and Ponemon Insitute, New York, NY.

Avizienis, A., Laprie, J.-C., Randell, B. and Landwehr, C.E. (2004), "Basic concepts and taxonomy of dependable and secure computing", *IEEE Transactions on Dependable and Secure Computing*, Vol. 1 No. 1, pp. 11-33.

Cervantes, G.V., Fenz S., *et al.* (2014), "How to assess confidentiality requirements of corporate assets?", in Null, N. C.-B. (Ed.), *29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco*, 2-4 June, Proceedings, IFIP International Federation for Information Processing, pp. 234-241.

Di Modica, G. and Tomarchio, O. (2016), "Matchmaking semantic security policies in heterogeneous clouds", *Future Generation Computer Systems*, Vol. 55, pp. 176-185.

Dobie, G. (Ed.) (2018), "Allianz risk barometer 2018", available at: www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2018/

Fenz, S. and Ekelhart, A. (2009), "Formalizing information security knowledge", *ASIACCS'09, Sydney, NSW*, 10-12 March.

Fenz, S., Ekelhart, A. and Neubauer, T. (2011), "Information security risk management: in which security solutions is it worth investing?", *Communications of the Association for Information Systems*, Vol. 28.

Fenz, S., Plieschnegger, S. and Hobel, H. (2016), "Mapping information security standard ISO 27002 to an ontological structure", *Information and Computer Security*, Vol. 24 No. 5.

Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014), "Current challenges in information security risk management ", *Information Management and Computer Security*, Vol. 22 No. 5, pp. 410-430.

Herzog, A., Shahmehri, N. and Duma, C. (2007), "An ontology of information security", *International Journal of Information Security and Privacy*, Vol. 1 No. 4, pp. 1-23.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design science in information systems research MIS Q", *Society for Information Management and the Management Information Systems Research Center*, Vol. 28, pp. 75-105.

ISO/IEC 27002 (2013), "Information technology – security techniques – code of practice for information security controls"

Karyda, M., Balopoulos, T., Gymnopoulos, L., Kokolakis, S., Lambrinoudakis, C., Gritzalis, S. and Dritsas, S., (2006), *An ontology for secure e-government applications ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)*, *IEEE Computer Society*, pp. 1033-1037.

Kim, A., Luo, J. and Kang, M., (2005), "Security ontology for annotating resources", *OTM Conferences (2)*, pp. 1483-1499.

Martimiano, A.F.M. and Moreira, E.S. (2005), "An owl-based security incident ontology", *Proceedings of the Eighth International Protege Conference*.

Neubauer, T., Ekelhart, A. and Fenz, S. (2008), "Interactive selection of ISO 27001 controls under multiple objectives", *Proceedings of The Ifip Tc 11 23rd International Information Security Conference Volume 278 of the series IFIP – The International Federation for Information Processing*, pp. 477-492.

OECD (2012), "Cybersecurity policy making at a turning point", Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy, No.: 211, doi: 10.1787/5k8zq92vdgtl-en.

Salini, P. and Shenbagam, J. (2015), "Prediction and classification of web application attacks using vulnerability ontology", *International Journal of Computer Applications*, Vol. 116 No. 21.

Schumacher, M., (2003), *Security Engineering with Patterns – Origins, Theoretical Model, and New Applications*, Springer, Berlin.

Solic, K., Ocevcic, H. and Golub, M. (2015), "The information systems' security level assessment model based on an ontology and evidential reasoning approach", *Computers and Security*, Vol. 55, pp. 100-112.

Souag, A., Mazo, R., Salinesi, C. and Comyn-Wattiau, I. (2015), "Reusable knowledge in security requirements engineering: a systematic mapping study", *Requirements Engineering Journal*, Vol. 21, pp. 1-33.

Further reading

Fenz, S. (2010), "From the resource to the business process risk level", in Clarke, N., Furnell, S. and von Solms, R. (Eds), *12th Annual IFIP Workshop on Information Security Management – Proceedings of the South African Information Security Multi-Conference (SAISMC'2010)*, pp. 100-109.

Fenz, S., Ekelhart, A. and Neubauer, T. (2009), "Business process-based resource importance determination", *Proceedings of the 7th International Conference on Business Process Management (BPM'2009)*, *Springer*, pp. 113-127.

Fenz, S., Neubauer, T., Accorsi, R. and Koslowski, T. (2013), "FORISK: formalizing information security risk and compliance management", *Annual IEEE/IFIP International Conference on Dependable Systems and Networks*.

Corresponding author

Stefan Fenz can be contacted at: stefan.fenz@tuwien.ac.at