Communications of the Association for Information Systems

Volume 28 Article 22

5-2011

Information Security Risk Management: In Which Security Solutions Is It Worth Investing?

Stefan Fenz
Vienna University of Technology, Austria, stefan.fenz@tuwien.ac.at

Andreas Ekelhart
SBA Research, Austria

Thomas Neubauer
Vienna University of Technology, Austria

Communications of the Association for Information Systems

CAIS

Information Security Risk Management: In Which Security Solutions Is It Worth Investing?

Stefan Fenz

Vienna University of Technology, Austria

stefan.fenz@tuwien.ac.at

Andreas Ekelhart

SBA Research, Austria

Thomas Neubauer

Vienna University of Technology, Austria

Abstract:

As companies are increasingly exposed to information security threats, decision makers are permanently forced to pay attention to security issues. Information security risk management provides an approach for measuring the security through risk assessment, risk mitigation, and risk evaluation. Although a variety of approaches have been proposed, decision makers lack well-founded techniques that (1) show them what they are getting for their investment, (2) show them if their investment is efficient, and (3) do not demand in-depth knowledge of the IT security domain. This article defines a methodology for management decision makers that effectively addresses these problems. This work involves the conception, design, and implementation of the methodology into a software solution. The results from two qualitative case studies show the advantages of this methodology in comparison to established methodologies.

Keywords: risk management**,** cost benefit analysis, decision support system, expert system

Volume 28, Article 22, pp. 329-356, May 2011

The manuscript was received 12/11/2009 and was with the authors 7 months for 3 revisions.

I. INTRODUCTION

As almost every business decision is based on data, reliable information technology (IT) is a prerequisite for business continuity and, therefore, crucial for the entire economy [Gerber and von Solms, 2004; Commission of the European Communities, 2006]. The importance of information technology brought with it the urgent need to ensure its continuous and reliable operation and to protect the processed and stored information. Recent research has shown the impact of security breaches on the market value of organizations. Organizations lost an average of approximately 2.1 percent of their market value within two days surrounding security breaches [Cavusoglu et al., 2004a]. The interconnectedness of the global economic system enables information security threats such as computer viruses to proliferate with great speed. Even though the connection of almost every organization to the Internet and the spread of computer viruses represent only two vulnerabilities and potential information security risks for organizations, they still illustrate the changes in the threat environment over the last decades [cf. Bagchi and Udo, 2003] and the reasons why organizations should strive to manage these risks adequately. In general terms, risk is defined as *the probability per unit time of the occurrence of a unit cost burden* [Sage and White, 1980]. In the information security context, risk is defined as *a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization* [Stoneburner et al., 2002]. As the security measures necessary to lower the risk are almost always associated with costs, organizations seek measures that are capable of reducing the risk to an acceptable level at the lowest possible cost. Information security risk management addresses exactly these issues and was defined by the National Institute of Standards and Technology (NIST) in Special Publication 800-30 as *the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions* [Stoneburner et al., 2002]. Information security risk management is a crucial element in ensuring long-term business success. Experts have proposed numerous approaches to implementing an adequate information security risk management strategy.

Regardless of which information security risk management methodology is considered, it always includes the assessment of business-critical assets of potential threats, vulnerabilities, and measures that can reduce the risk to an acceptable level [Baskerville, 1993]. While in-depth knowledge of the organization in question and the information security domain as a whole is fundamental to the presented approaches [Jung et al., 1999], little research has been conducted on the formal knowledge representation of the domains that are relevant to information security risk management [cf. Schumacher, 2003; Kim et al., 2005; Herzog et al., 2007]. Recent studies [e.g., Straub and Welke, 1998] have shown that the lack of information security knowledge at the management level is one reason for inadequate or nonexistent information security risk management strategies, and that raising the management's level of information security awareness and knowledge leads to more effective strategies. Smith and Spafford [2004] and PITAC [2005] identified information security risk management as one of the top ten grand challenges in information technology security and called for sound theories and methods to support and improve existing information security risk management approaches. In 2006, the European Network and Information Security Agency (ENISA) addressed these issues [cf. ENISA, 2006] and rated the establishment of unified information bases for information security risk management and the development of risk measurement methods as high priority issues. Only a short time later, Aime et al. [2007] confirmed the lack of a set of well-defined formal models for supporting the information security risk management process. Only 48 percent of 1,007 interviewed UK organizations formally assess information security risks (2008 Information Security Breaches Survey [BERR, 2008]). To date such organizations have mostly relied on best practice guidelines, information security standards, and/or domain experts to conduct the risk assessment and mitigation phases.

However, these approaches have several problems:

- Domain expert dependence: best practice guidelines provide excellent knowledge about potential threats, vulnerabilities, and controls, but without an information security domain expert, the organization is not always able to consider the numerous complex relationships between all the relevant information security concepts. The result is a non-holistic information security approach, which endangers the performance of the organization's mission [Vitale, 1986; Bandyopadhyay and Mykytyn, 1999; Jung et al., 1999; Baker and Wallace, 2007].

- Manual threat—infrastructure mapping: to identify concrete infrastructure elements that are endangered by certain threats, the organization has to manually match the knowledge gained from best practice guidelines to their actual infrastructure [Baskerville, 1993].

- Abstract implementation suggestions: information security standards frequently only include very abstract implementation suggestions for risk mitigation. Usually there are few or no concrete suggestions for controls, leading to inefficient risk mitigation strategies [Baker et al., 2007].

- Subjective threat probability determination: the determination of threat probabilities is predominantly based on subjective perceptions and not on an objective evaluation [Frosdick, 1997; Bandyopadhyay and Mykytyn, 1999; Baker et al., 2007].

- Unquantifiable IT security solution effectiveness: while companies strive for cost-conscious solutions, they are frequently unaware of their volume of investment in IT security and/or, even more importantly, whether these investments are effective [Ittner and Larcker, 2003; Smith and Spafford, 2004].

- No interactive decision support: management decision makers, such as the CPO or CIO, have to cope with the task of selecting the most appropriate set of IT security investments from a great spectrum of potential IT security investments. The results of existing methods provide decision makers with inadequate or little intuitive and/or interactive decision support and, as a result, do not support them in identifying an appropriate risk versus cost trade-off when investing in IT security solutions [Lander and Pinches, 1998].

Research Objectives and Approach

This research elaborates on existing information security risk management approaches and identifies the problems that typically arise in the implementation of these approaches. The goal is to address the identified problems and to provide methods that enable management decision makers to deal effectively with the following problems:

- RQ1: How can we comprehensibly calculate information security standard-compliant IT security solution portfolios?

- RQ2: How can we effectively communicate the portfolios' risk versus cost trade-off figures to management decision makers?

In order to answer the posed research questions and to provide the contributions described in the following section, the research project uses a combination of conceptual-analytical, artifact-building, and artifact-evaluating research approaches [Järvinen, 2000]. Therefore, this article starts with a detailed exploration of existing information security risk management methodologies. We do this by comparing and analyzing related work (conceptual-analytical approach). The requirements defined in this article are based on the results of the literature research and the identified shortcomings. A further section deals with the development of novel techniques, the extension and improvement of existing techniques, and the application of these techniques to the information security risk management domain (artifact-building and artifact evaluation). Finally, the research results were validated with the design and implementation of a prototype and by conducting case studies in two small and medium-sized European enterprises.

This research makes a contribution to the literature in the field of qualitative and quantitative information security risk management with an emphasis on decision support. To the best of our knowledge it is the first scientific effort for a comprehensive improvement of the automation and comprehensibility of the entire risk management process. Existing work in the field addresses sub-problems [cf. Finne, 1998a; Finne, 1998b; Gordon and Loeb, 2002; Arora et al., 2004; Cavusoglu et al., 2004b; Bodin et al., 2008] or provides high-level theoretical risk management frameworks [cf. Farquhar, 1991; Stoneburner et al., 2002; Fredriksen et al., 2002; Alberts et al., 2003; DCSSI, 2004; ISO/IEC, 2007]. Our AURUM ("AUtomated Risk and Utility[1] Management") framework, in comparison, supports organizations throughout the entire risk management process by:

- using a novel information security ontology to provide best practice knowledge regarding threats, vulnerabilities, controls, potential control implementations, and asset classes

[1] Referring to http://wordnet.princeton.edu, we define *utility* as a measure that is to be maximized in any situation involving choice.

- automatically calculating the importance of business-critical assets based on their involvement in business processes and the overall importance of these processes
- automatically determining threat probabilities based on the organization-specific threat environment and existing control implementations
- using reasoning engines and the ontology to automatically determine control implementation gaps and potential control implementations that can be used to fill these gaps
- providing novel multi-objective decision support methods to interactively select control implementation portfolios based on existing control implementations

The comparison with similar risk management tools carried out in two case studies shows that AURUM provides the following unique benefits to management decision makers: (1) reduced domain expert dependence, (2) automatic threat–infrastructure mapping, (3) concrete control implementation suggestions, (4) objective threat probability determination, (5) measurable IT security solution effectiveness, and (6) interactive decision support in IT security solution portfolio selection.

II. BACKGROUND

Risk management in the context of information technology is not a new research domain. In 1975 the U.S. National Bureau of Standards proposed the Annual Loss Expectancy (ALE) as a metric for measuring computer-related risks [FIPS, 1975]. ALE is calculated by summing up the products of impact ($I(O_i)$) and frequency (F_i) of harmful outcomes $(O_1,...,O_n) \rightarrow ALE = \sum_{i=1}^{n} I(O_i)F_i$. One shortcoming of this early approach is the fact that it does not distinguish between highly frequent, low impact events and rare, high impact events. In the 1980s it was again the U.S. National Bureau of Standards that advanced efforts in the information security risk management domain [Soo Hoo, 2000]. In a series of workshops they developed an iterative process for information security risk management that consists of the following steps: (1) identification of the requirements (asset values, threats, vulnerabilities, existing controls, etc.), (2) analysis of threats, vulnerabilities, and the scenario, (3) risk measurement, (4) acceptance test, and (5) control selection and implementation [Soo Hoo, 2000]. Although the information security risk management approaches of the following years provided some additional steps or different process structures, they are based mainly on that approach developed in the 1980s. A combination of qualitative and quantitative risk analysis methodologies was proposed by Rainer et al. [1991]. It consists of the following steps: identification of organizational value activities, identification of the IT component of each value activity, identification of linkages among value activities and the IT components that support each of them, determination of IT assets that support interorganizational linkages, determination of the value of IT assets, identification of possible threats, identification of the vulnerability of assets to threats, and determination of the overall IT risk exposure. The security risk planning model by Straub and Welke [1998] includes the recognition of security problems, risk analysis (threat identification and risk prioritization), alternatives generation (generation of solutions that can mitigate the risk), decisions (selection and prioritization of security projects), and implementation. In addition to the general risk management frameworks, a number of information security investment decision support methods, which are an integral part of several information security risk management methodologies, have been proposed [cf. Finne, 1998a; Finne, 1998b; Gordon and Loeb, 2002; Arora et al., 2004; Cavusoglu et al., 2004b]. In 2008, the PCR (perceived composite risk) metric was introduced by Bodin et al. [2008]. Their approach extends the traditional ALE by combining it with the expected severe loss and the standard deviation of the loss, and provides organizations with an additional decision support tool for information security investments. To make these academic approaches usable to organizations, some of them were used as a foundation for today's information security risk management methods, standards, and best practice guidelines (e.g., CRAMM [Farquhar, 1991], NIST SP 800-30 [Stoneburner et al., 2002], CORAS [Fredriksen et al., 2002], OCTAVE [Alberts et al., 2003], EBIOS [DCSSI, 2004], and recently ISO 27005 [ISO/IEC, 2007]).

III. AURUM: A FRAMEWORK FOR AUTOMATED INFORMATION SECURITY RISK MANAGEMENT

Best practice guidelines, information security standards, and expert knowledge can support organizations in the risk assessment and mitigation phases, but have a variety of shortcomings. Regardless of which of the existing support approaches is used, every organization has to invest a great deal of time and money in manually dealing with the following questions, among others:

1) What are potential threats for my organization?

2) How probable are these threats?
3) Which vulnerabilities could be exploited by such threats?
4) Which controls are required to most effectively mitigate these vulnerabilities?
5) What is the potential impact of a particular threat?
6) What is the value of security investments?
7) In which security solutions is it worth investing?

Our research focuses on developing concepts to meet these demands of the information security risk management (ISRM) community with the aim to support risk managers in making efficient security decisions, thereby protecting the organization's mission. The detailed specification of the developed concepts introduces new automated risk management approaches. Figure 1 shows how our contributions support the main ISRM-phases. The purpose of the entire framework is to support investment decision makers in interactively selecting efficient security solutions. The following itemization briefly outlines the underlying approaches:

1) Business Process Importance Determination: The ISRM process starts with the business process importance phase. AURUM automatically calculates importance values for assets that are required by the activities of the process. It bases the calculations on existing business process models and an overall importance value for each process. The results of this calculation indicate the overall impact on the organization should the asset not be available.

2) Inventory Phase: In the inventory phase, AURUM supports organizations in defining (i) their assets, (ii) the acceptable risk level for the defined assets, (iii) the organization-wide importance of these assets, and (iv) attacker profiles in terms of motivation and capability. Assets (e.g., servers and data) are obtained (i) automatically in the business process importance determination phase based on existing business process models, and/or (ii) manually in the inventory phase by mapping the infrastructure of the organization to the ontological knowledge base. We developed a security ontology in order to store and interlink this information with general information security domain knowledge.

3) Threat Probability Determination: In the threat probability phase, the Bayesian threat probability determination developed by us uses the security ontology to extract knowledge regarding threats and their a priori probabilities, vulnerabilities, existing and potential control implementations, attacker profiles, and the assets of the organization. With this knowledge, it establishes a Bayesian network capable of calculating threat probabilities based on the aforementioned input information.

4) Risk Determination: In the risk determination phase, relevant threat probabilities are merged with the importance information for each asset.

5) Control Identification and Evaluation: In this phase, existing and potential control implementations and their attributes are extracted from the security ontology to support the developed interactive multi-criteria decision support methodology. With this, we provide a solution concept for two fundamental ISRM questions: (i) Which IT security solutions can generally be used to mitigate the risk to an acceptable level?, and (ii) Which IT security solutions should be used to mitigate the risk to an acceptable level in a cost-efficient way?

The following subsections describe our approach to address these questions in detail.

Business Process Importance Determination

Input	Business Processes, connected Assets and the Business Process Value
Artifact	Business Process Importance Determination Algorithm
User Interaction	None
Output	Assets and their importance values

The first step in our framework addresses the determination of asset importance values. Based on the definitions in NIST 800-30, the importance indicates the organizational impact if the considered asset is no longer able to conduct its designated tasks.

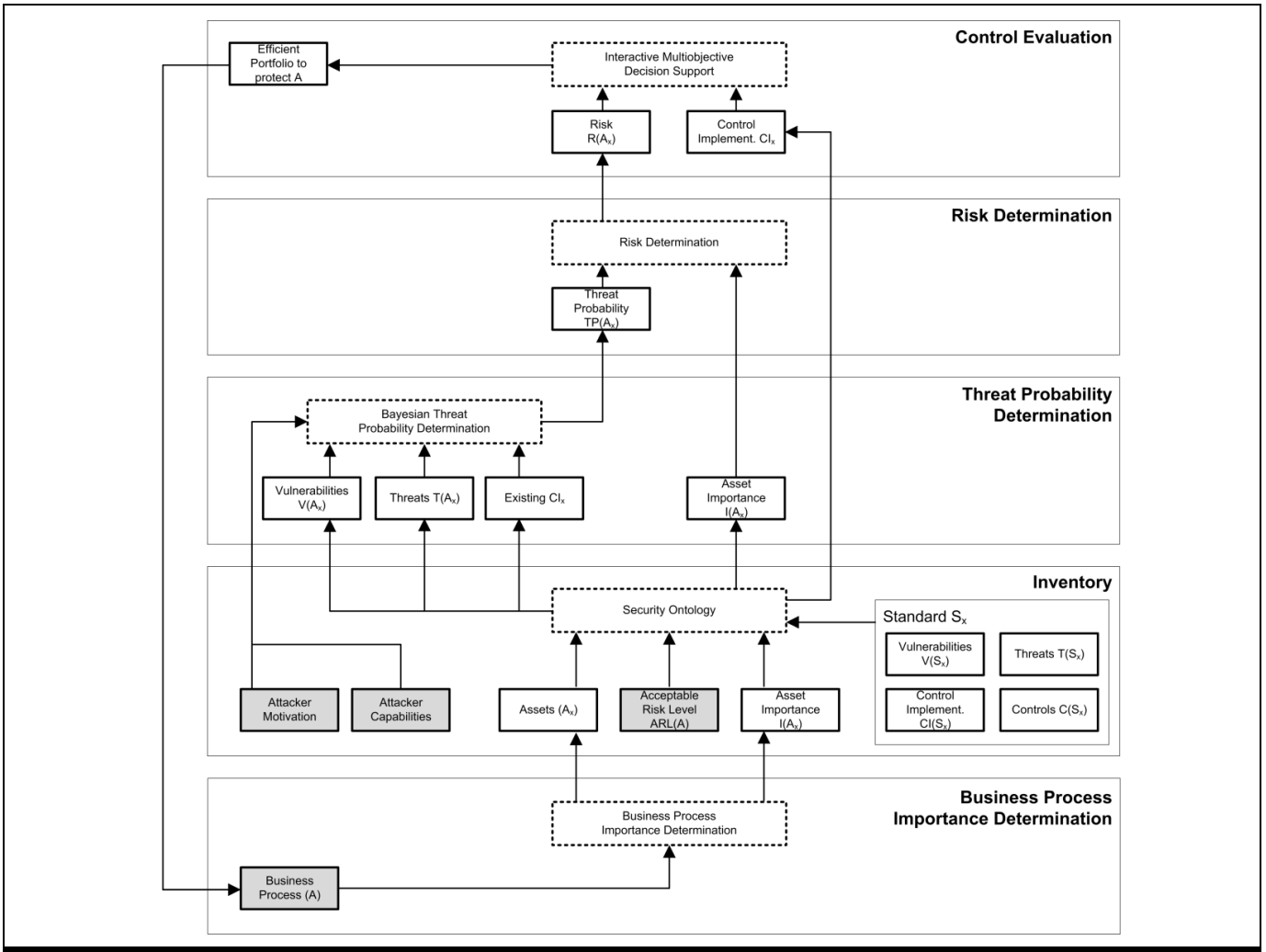

Figure 1. AURUM Architecture

Even though a great deal of research was conducted and numerous ISRM approaches were developed in the past thirty years, this data is still mostly gathered manually. This makes it a work-intensive process that relies on interviews and questionnaires with system and information owners. Due to the identified shortcomings of existing approaches, and the recurring nature of this step, we developed a methodology [cf. Fenz, Ekelhart and Neubauer, 2009] to automatically determine asset importance values through business process analysis. The following paragraph briefly outlines how we use the method in the context of information security risk management.

Our method requires business process models as input, including required assets connected at the activity level, which are internally transformed into Petri nets for further processing. Currently, we have parsers for ADONIS, but due to the usage of Petri nets as analysis basis, other BPM formats could be integrated easily. If business process documentation is not already available in an organization, business process analysis has to be conducted in advance. In addition, an importance value has to be assigned to each business process, either monetary (e.g., Euros per hour) or qualitative (e.g., High, Medium, and Low). With this input data, our method calculates two values for each resource: (1) a business process-wide, local importance value and (2) an organization-wide, global importance value. First, local importance values are calculated for each process activity assuming a uniform distribution regarding potential process execution flows. To calculate the local importance value of a resource, the activity with the highest importance that uses the resource in question is selected and multiplied by the overall importance of the business process. Finally, the global resource importance is calculated by summing up all local importance values. The advantages of this asset importance determination approach are: (1) the necessary input data is restricted to machine-interpretable business process representations including required resources and the importance of the business process, and (2) assuming that the required input data is already available, our approach provides ISRM with fast results for resource importance, which are based on the business processes' structure and resource involvement. Details on this approach can be found in Fenz, Ekelhart and Neubauer [2009]. At the moment, the automatic importance determination addresses only the security attribute availability. Impact values for integrity and confidentiality can be assigned manually for each asset.

Inventory

Input	Assets, their acceptable risk level and importance
Artifact	Security Ontology
User Interaction	Mapping the infrastructure of the organization to the security ontology
Output	Security Ontology including the organization's assets

ISRM requires the detailed definition of the system boundaries, assets, and information used and/or required by the system under analysis. This includes the systematic inventory of hardware, software, existing physical and organizational controls, system interfaces, data, information, and persons who support or use the IT system. One of the fundamental but unsolved requirements in modern information security risk management is a common language that provides a shared understanding and communication basis for all involved parties. Such a language should not only include elaborate term definitions, but also addresses the context in which terms can be connected. With respect to machine-readability, ontologies are a reasonable solution for these requirements ([cf. Gómez-Pérez et al., 2004], for the advantages of a formal specification).

Our security ontology [cf. Fenz and Ekelhart, 2009] is based on the security relationship model presented in the National Institute of Standards and Technology Special Publication 800-12 [NIST, 1995]. The application of the security ontology to ISRM contributes to this area in the following way: (1) Ontologies facilitate interoperability by providing a shared understanding of the domain in question and help to avoid heterogeneity, (2) they provide a formalization of shared understanding which allows machine processability, and (3) they allow the reuse of information already gathered within the company. Not only can the created data be reused in future projects, independently of implemented tools, but other groups, e.g., open communities facing similar risks in the same domain or partner organizations, profit from the collected data as well.

Figure 2 shows the high-level concepts and relations of the security ontology, in which threats, vulnerabilities, controls, and their implementations are the pivotal elements. As soon as a threat exploits a physical, technical, or administrative weakness, it gives rise to follow-up threats, represents a potential danger to the organization's assets, and affects specific security attributes (e.g., confidentiality, integrity, and/or availability). We also use potential threat origins (human or natural origin) and sources (accidental or deliberate source) to describe each threat. Each vulnerability is assigned a severity value and the asset on which it could be exploited. Decision makers have to implement controls to mitigate an identified vulnerability and to protect the respective assets through preventive, corrective, deterrent, recovery, or detective measures (control type).

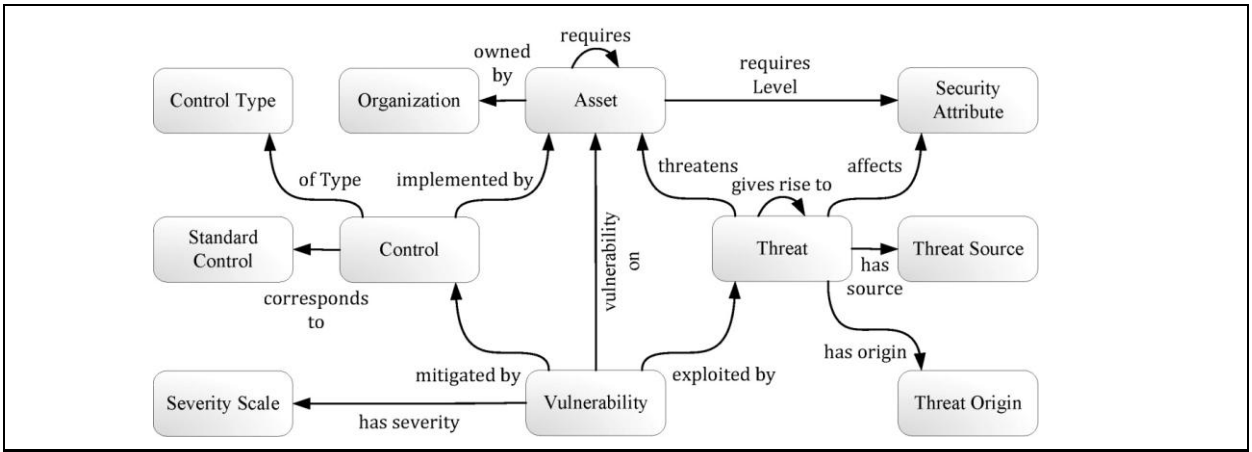

Figure 2. Security Concepts and Relationships

Each control is implemented as an asset concept, or as a combination of several asset concepts. We derived our controls from, and specified them to correspond with, best practice and information security standard controls (e.g., the German IT Grundschutz Manual [BSI, 2004] and ISO/IEC [2005]) to ensure the incorporation of widely accepted knowledge. The controls are modeled on a highly granular level and are thus reusable for different standards. When implementing the controls, compliance with various information security standards is implicit. The coded ontology follows the OWL-DL (W3C Web Ontology Language) [W3C, 2004] standard and ensures that the knowledge is represented in a standardized and formal way to enable automated systems to use it. Note that Figure 2 shows only the framework from a high level perspective. Visit http://sec.sba-research.org to see the full and latest version of the security ontology. One important concept not included in Figure 2 is the probability concept (sec:Probability), which

assigns each threat a location-dependent a priori probability. Domain experts estimate these probabilities based on statistical data (e.g., historical weather data or local crime reports). Information on a priori probabilities has to be provided only once and can be reused by all users located in the same area.

A complete and accurate model of the organization would be the ideal information security risk management basis. The introduced security ontology already incorporates an elaborate set of concept definitions, relations, and formal axioms to generate an ontological model of the organization in the inventory phase. Although a complete model of the organization's environment is desirable, users can also model specific parts of interest only.

Threat Probability Determination

Input	Security Ontology including the organization's assets
Artifact	Bayesian Threat Probability Determination
User Interaction	None
Output	Asset-specific threat probabilities

A threat requires a threat origin and an existing vulnerability to become effective. A human threat origin can exploit a vulnerability either accidentally or deliberately. In this step it is important to compile a comprehensive list of potential threats as recommended in Stoneburner et al. [2002]; DCSSI [2004]; BSI [2004], because the subsequent risk determination step uses the results of this step as input for the risk mitigation strategy. While standards and best practices often provide an example threat list, the risk manager is not always familiar with the nature of each threat. Which threats endanger critical assets? Which threat is a multiplier (i.e., gives rise to other threats)? Which vulnerabilities does a threat have to exploit to become effective? Most current information security risk management standards or best practice guidelines hardly address these questions. Therefore, in order to identify potential threats against the inventoried system, we use the security ontology, which includes information on threats and their relationship to asset concepts. By inspecting each threat definition and following the formal sec:threatens relationship, it is possible to identify all threatened asset concepts. In a next step, all organization specific assets, which were modeled in the inventory phase, can be retrieved by querying instances of the threatened classes. As a result, we receive a list of potential threats and the corresponding organization's assets that are at risk.

Starting from the threat report produced in the previous step, the vulnerability identification step analyzes potential vulnerabilities that are present in the defined system. For each threat, highly granular vulnerabilities that it could exploit is defined and modeled in the ontology. A description of each vulnerability in natural language complements the vulnerability presentation. For each of the vulnerabilities, the security ontology provides mitigation controls. Each control is enriched by a natural language description to make it easier to understand. With these functions in place, a user knows exactly how to protect the organization from specific threats: mitigating vulnerabilities by implementing recommended controls. After this step, the organization has good knowledge of the system in question, potential threats, and corresponding vulnerabilities that allow threats to become effective.

In the next step, the probability determination is concerned with the probability that a threat exploits a certain vulnerability within the given system. Therefore, the organization has to deal with the following factors: (1) motivation and capability of the threat agent in the case of deliberate threat origin, (2) vulnerability type, and (3) effectiveness of existing control implementations. We used the following approach to establish a threat probability calculation schema based on the security ontology to obtain asset and organization-specific threat probabilities (see Figure 3 for a schematic representation): (1) We query the security ontology to obtain those threats that directly threaten the asset in question (*sec:Threat sec:threatens ent:Asset*). (2) We obtain the predecessors of each threat recursively in order to generate an asset-specific threat net (*sec:Threat sec:canBeConsequenceOf sec:Threat*). (3) We determine the corresponding vulnerabilities for each threat in the established threat net (*sec:Threat sec:exploits sec:Vulnerability*). (4) We determine the controls that are able to mitigate each vulnerability (*sec:Vulnerability sec:mitigatedBy sec:Control*). (5) For each control, we determine the inventoried assets that are able to protect the considered asset as per the formal control implementation specification. After setting up the threat probability determination net by querying the ontological relations and concepts, the asset-specific threat probability of a specific threat can be calculated using the following calculation schema (bottom-up):

1) Vulnerability-specific (V_i) attacker effectiveness *AE* taking weighted attacker capability *AC* and motivation *AM* into account (cf. Equation 1).

2) Weighted and vulnerability-specific effectiveness of existing control implementations CCE_{Vi} (cf. Equation 2).

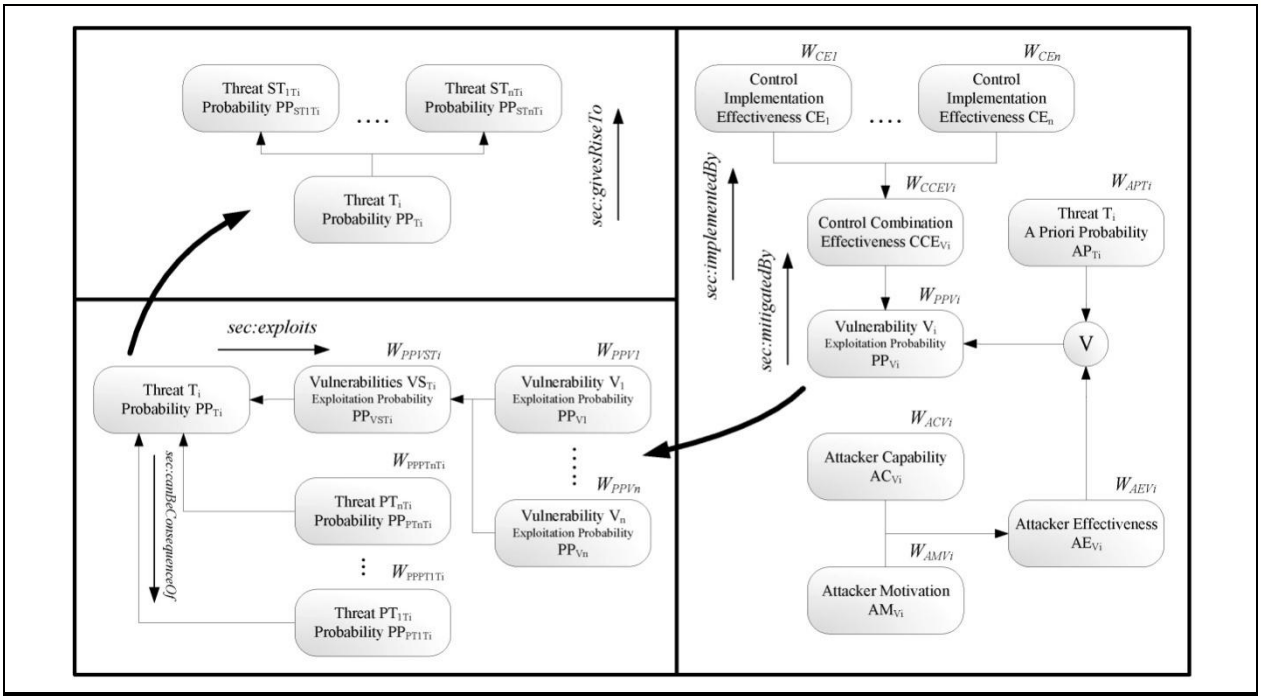

Figure 3. Threat Probability Calculation Schema

3) Vulnerability exploitation probability PP_{Vi} .

   a. determined by attacker effectiveness AE_{Vi} in case of deliberate threat sources (cf. Equation 3).

   b. determined by a priori probability AP_{Ti} of the corresponding threat T_i in case of accidental threat sources (cf. Equation 4).

4) Vulnerabilities' exploitation probability PP_{VSTi}. Summarizes the exploitation probability ratings of its parents PP_{Vi} to decrease the probability calculation's complexity in the subsequent PP_{Ti} variable (cf. Equation 5).

5) Threat probability PP_{Ti} taking weighted vulnerability PP_{VSTi} and predecessor threat probabilities PP_{PTjTi} into account (cf. Equation 6).

$$AE_{Vi} = AC_{Vi} * W_{AC_{Vi}} + AM_{Vi} * W_{AM_{Vi}} \quad (1)$$

$$CCE_{Vi} = \sum_{i=1}^{n} (CE_i * W_{CEi}) \quad (2)$$

$$PP_{Vi} = CCE_{Vi} * W_{CCE_{Vi}} + AE_{Vi} * W_{AE_{Vi}} \quad (3)$$

$$PP_{Vi} = CCE_{Vi} * W_{CCE_{Vi}} + AP_{Ti} * W_{AP_{Ti}} \quad (4)$$

$$PP_{VSTi} = \sum_{i=1}^{n} (PP_{Vi} * W_{PP_{Vi}}) \quad (5)$$

$$PP_{Ti} = PP_{VS_{Ti}} * W_{PP_{VSTi}} + \sum_{j=1}^{n} (PP_{PT_{jTi}} * W_{PP_{PTjTi}}) \quad (6)$$

If threat T_i is connected to any successor threats (e.g., asset loss would be a successor threat of theft), it influences their threat probability. The state of each node (N) in the Bayesian network (see Figure 3 for a schematic representation) is determined by the numerical state of its predecessors (N_{pi}) and their corresponding weights:

$$N = \sum_{i=1}^{n} (N_{pi} * W_{N_{Pi}}) \quad (7)$$

By default and except for the vulnerability nodes, all nodes in the Bayesian network are weighted equally. We used best practice vulnerability severity ratings to derive the weight for each vulnerability node. Note that each threat probability is calculated for each asset, since the determination of already implemented controls is always bound to

the considered asset. To get a specific threat probability over the entire organization, the individual threat probabilities per asset have to be aggregated. Thus, our approach enables the risk manager to deal both with overall and asset-specific risks, as necessary. The main advantage of the proposed Bayesian threat probability determination is that it gives the risk manager a way to determine the threat probability in a structured and comprehensible way. The calculation schema is fully documented and each state of the Bayesian network can be explained and justified mathematically and formally taking the given input factors into consideration. In addition to the Bayesian calculation schema, the security ontology is used to enrich the Bayesian network with concrete and up-to-date information security domain knowledge (e.g., newly discovered vulnerabilities). See Fenz, Tjoa and Hudec [2009] and Fenz and Neubauer [2009] for a detailed description of how the Bayesian network was derived from the security ontology and how the final threat probabilities are calculated. To see the entire Bayesian threat probability determination network, go to http://securityontology.sba-research.org/network.zip. The freely available Norsys Netica application is required to open, view, and use the network, which shows threats, vulnerabilities, a priori probabilities for threats, control implementations, and attacker profiles for 557 nodes, 579 directed links, and 30,687 conditional probabilities. Understanding the adverse impact of a successful exploitation of a vulnerability by a threat, the risk level must be determined, which forms the basis for the subsequent control recommendations. While in most risk assessment approaches, such as proposed in Stoneburner et al. [2002], Burtles [2007], Peltier [2005], Kairab and Kelly [2004], the impact of threats is determined through interviews and workshops involving the system and information owners, our approach focuses on an automated support using the developed knowledge base and the defined relationships.

Risk Determination

Input	Threat probability and importance of the asset
Artifact	Risk calculation
User Interaction	None
Output	Risk level of the considered asset

In the next step we assess the adverse impact of a specific threat. Due to the semantic relations between a threat and threatened asset classes, we automatically obtain a collection of concrete threatened assets in an organization (taken from the inventoried assets, cf. Section Inventory). The security attribute put at risk by a threat is added to the description of each threat. We then compare the security attribute at risk, gained from the threat, with the impact categories defined for each threatened asset. Note that we always calculate the risk for threat/asset pairs, as the impact might be different for each asset. If a security attribute affected by the threat is defined as relevant (impact on loss of the security attribute has been rated) for a threatened asset, impact on the organization owning the asset must be expected. To determine the magnitude of impact, we apply the assigned impact level to the asset.

The following example illustrates the impact determination in case of a threat occurrence: The threat of a computer virus puts the security attribute “availability” at risk. A file server, located in the organization, was automatically assigned an impact value of High in case of unavailability (cf. Section Business Process Importance Determination). Due to the relationship between threats and assets, we know that the server is threatened by the computer virus. Comparing the information shows that the server’s availability is threatened, and with it the organization. Because the impact is set to *High* for event of the server being unavailable, we can expect a high impact on the organization in case of a computer virus attack. This result is exactly the impact level of the threat exposure. An important and common aspect to mention in this context is the case where more than one threatened asset is identified in the organization. I.e., if a threat is defined on the concept level and more than one instance of threatened asset concepts exists (e.g., more than one server in an organization), the overall threat impact level is defined by the highest impact level over all threatened assets. As a final step in risk determination, the mission risk is calculated by multiplying the ratings assigned to threat probability and the potential impact. The measurement unit of the final risk level depends on the measurement unit that is used for impact calculation. In AURUM the impact is calculated by using a continuous (e.g., monetary units) or discrete (e.g., high, medium, low) scale. The probability is a numerical value in the range of 0 to 100 (percentage value).

We now know the individual risk for every threatened asset in case a threat occurs. These asset-bound risk levels are required in the subsequent control recommendation step, as countermeasures could be required individually for each asset. While traditional methods are valuable, it is not clear which assets cause a risk level and where to apply countermeasures. Our approach, however, provides detailed insight, listing exactly which assets are endangered, what impact they cause and the threat’s probability. This makes it possible to understand the calculated risk figures. In addition, this approach allows decision makers to focus exactly on the assets that cause the highest risk and provide control recommendations automatically as shown in the following sections.

Control Identification and Evaluation

Input	Relevance of existing and potential control implementations, risk level of the considered asset, and existing and potential control implementations, their effectiveness, initial and running costs
Artifact	Multi-criteria decision support
User Interaction	Interactive changing of the criteria boundaries
Output	Efficient IT security portfolios

At this point management knows which risks are not acceptable for the organization and, therefore, have to be mitigated or eliminated through appropriate security measures. To support this recommendation step, we consult the security model. For each vulnerability, appropriate controls are modeled, taken from best practice standards such as the German IT Grundschutz Manual. In contrast to the traditional process, this solution provides a thorough knowledge base about countermeasures and, thus, (1) saves time, (2) prevents effective solutions from being overlooked or forgotten, and (3) provides effective controls in compliance with best practice standards. However, even with the list of potential control instances, the decision maker still has to identify the optimal set of security solutions that fits the budget and provides the expected benefits. Each control can be realized by a variety of control instances that not only have different values for protecting corporate assets, but also demand different assets for implementation. Cost/benefit analysis, which is sometimes carried out to support this decision, is rarely considered by existing information security risk management approaches such as NIST SP 800-30. Despite the importance of this step, NIST SP 80030 gives only a rough overview of how to perform this step. Of course, decision makers could carry out cost/benefit analysis anyway, but valuation methods that focus solely on financial aspects are often considered to be ill-suited for security investments, because they (unsurprisingly) fail to properly take into consideration the many important nonfinancial criteria [cf. Ittner and Larcker, 2003; Ryan and Gates, 2004].

Solving this problem involves identifying Pareto-efficient combinations (i.e., combinations where no other solution with equally good or better values in all K objectives and a strictly better value in at least one objective exists) of security solutions. The multiobjective combinatorial optimization problem (MOCO) lies in maximizing K objectives (such as risk reduction, availability, or reliability). Note that functions $u_k(x)$ may take any form (linear, nonlinear, etc.) as long as they are defined for all (feasible) alternatives x. The careful specification of resource and benefit categories is of vital importance as these categories should reflect the corporate strategy and security policy. The criteria can range from monetary quantities (e.g., the reduction of monetary loss, minimizing monetary costs) to intangible values (e.g., user acceptance, implementation hours, loss of reputation, or security specific values such as reliability or effectiveness). The first set relates to limited resources (e.g., initial costs or running costs). The second set ensures that a suitable number of security solutions from given control subsets is included in the list of feasible solutions.

Decision makers are often overwhelmed with the high number of alternative solution and often do not know whether their investments into security are fitting or effective at all. Therefore, we provide decision makers with an intuitive interface for the control evaluation that offers them information on the specific selection problem, while the system ensures that the solution chosen will be an efficient one. The decision makers learn about the consequences of their decisions and get information on the gap between the existing solution and the potential solutions in each category. To support decision makers in determining the set of security solutions that best fits their ideas and objectives out of the possibly several thousand Pareto-efficient alternatives identified in the previous step, we use a search-based procedure. It starts with an efficient portfolio of security solutions (control implementations) and allows the decision maker to iteratively navigate in the solution space toward more attractive alternatives until no “better” portfolio can be found. Please note that we limited the user interface to the minimum of information necessary for the decision maker to make an informed decision:

- Our approach [cf. Neubauer and Stummer, 2007] is based on interactive modifications of lower and upper bounds for one or more objectives. The decision support system starts by displaying K floating bars (cf. Figure 5) representing resource and benefit categories (such as costs or availability) that are assigned units (such as “euro” in the case of costs or “points” in the case of availability). Two movable horizontal lines with small arrows on one side represent lower and upper bounds and are intended to restrict the set of remaining solutions in a step-by-step manner (e.g., by raising the minimum bound in one of the objectives) or for expanding it (e.g., by relaxing one or more of the bounds again) depending on the decision makers’ preferences.

- For each objective (cf. Figure 4), the system provides information on what can be achieved by the efficient solutions. Those values are represented by small dark marks on the left-hand side that can visually grow

together to form vertical blocks. As objective values are independent of each other (at least to some degree), the resulting visual "segmentation" differs between the objectives.

- For each objective (cf. Figure 4), the system provides information on the alternatives that remain after the decision maker has made decisions in their interactive exploration of the solution space. The wider colored bars on the right-hand side indicate the range of objective values achievable by solutions that fulfill all aspiration levels set so far. Technically, these bars should be segmented by to the aforementioned dark marks. However, for the sake of maximum legibility they are displayed as solid bars.

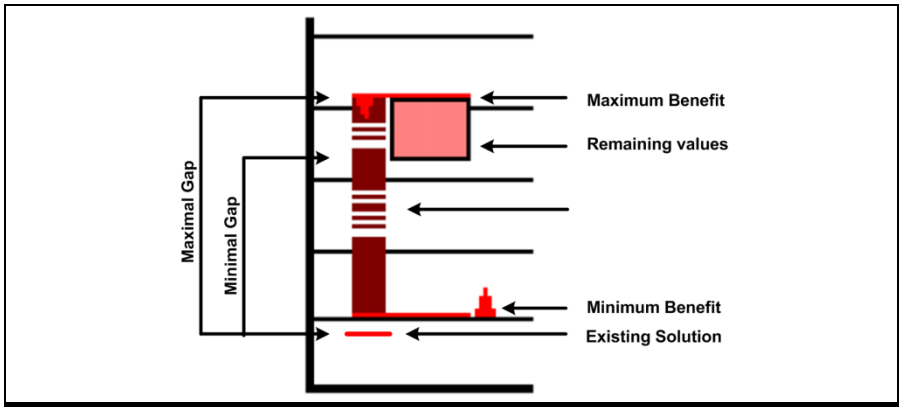

Figure 4. Subwindow Details

In all of these cases, the system provides immediate feedback about the consequences of such choices in terms of the remaining alternatives. We shall illustrate this by reducing the maximum level for Resource A (cf. Figure 6). Because this setting primarily filtered those solutions that come with a relatively high value in "Resource Category A" (and, on average, a somewhat higher need for Resource C) but still values in "Benefit Category A," the options in the other objectives were reduced as well and the position and size of the floating bars have changed accordingly. Raising the minimum value for Benefit A (e.g., functionality) narrows the set of remaining alternatives even further, since many alternatives with low resource values (e.g., costs) are excluded (cf. Figure 7).

In further iterations, the decision makers continue moving the minimum and maximum bounds and in doing so can learn about the consequences of their decisions and, thus, gain a much better idea of the issue in terms of what can be achieved in some objectives at what "price" in terms of opportunity costs in other objectives. After several cycles of restricting and once again expanding the opportunity set, the decision maker will finally end up with a solution that offers an individually satisfying compromise between the relevant objectives. Note that decision makers do not need to explicitly specify weights for objectives nor specify the form of their preference function or state how much better they consider one solution compared to another during any stage of the whole process. Instead, ample information on the specific selection problem is provided to them and the system ensures that the finally selected solution will be an optimal (i.e., Pareto-efficient) one, with no other feasible solution available that would be "better" from an objective point of view.

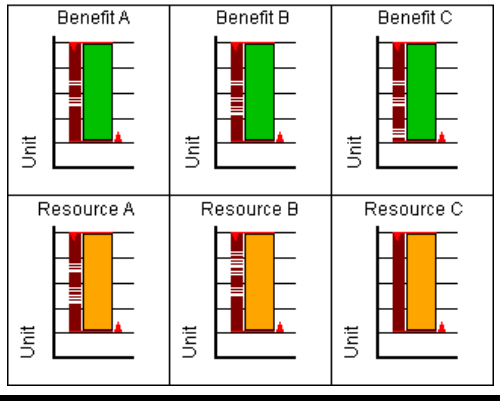

Figure 5. Initial Status

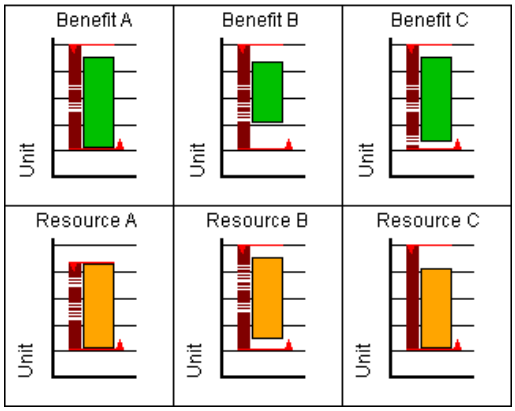

Figure 6. Status After the First Setting

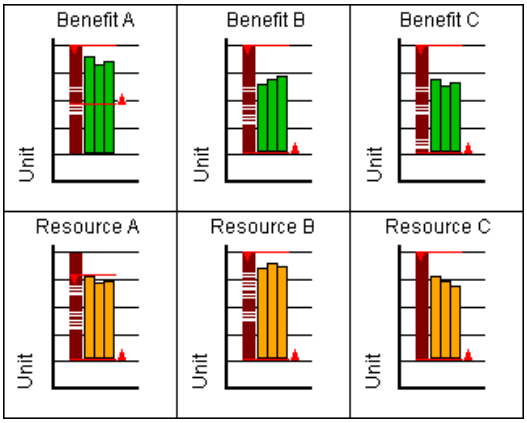

Figure 7. Status After Two Settings

IV. CASE STUDY

In order to empirically study the research propositions stated at the beginning of this article, we conducted two qualitative studies in small and medium-sized European enterprises (see Table 1). Due to the fact that security is an extremely sensitive issue for most enterprises, the identities of both organizations are withheld. In these case studies we conducted a risk assessment using the AURUM methodology developed by us.

Table 1: Conducted Case Studies

Number	Company	Department/Focus
1	Company A	Finance and Controlling
2	Company B	Server Infrastructure

Company A offers software development services and Company B specializes in information technology security consulting services. While both companies have an IS department, Company B expressed a substantially higher demand for information security due to their clientele and their rigorous nondisclosure agreements. In both companies we implemented the risk management approach with the support of the top management in cooperation with the IS department. In Company A we analyzed the Finance and Controlling department within two months, and in Company B the analysis took one and a half months. We used the AURUM methodology in both companies to check their ISO 27001 compliance and to recommend efficient control implementation portfolios.

In the following sections we present a more detailed overview of applying our AURUM approach in Case Study 1, where we followed the methodology described in this article. Details of the second case study are mentioned for the sake of comparison where necessary. AURUM was designed to minimize the interaction necessary between user and system and to provide decision makers with an intuitive solution that can be used without extensive knowledge of the information security domain. The reader should note that it would have been possible to start with the Business Process Importance Determination phase as shown in Figure 1 and afterwards inventory the rest of the environment.

Inventory

The basis of our information security risk management methodology is an accurate model of the organization described in the ontology. Section Inventory outlines the process of creating an ontological model of an organization from scratch. We modeled the department environment based on the input of the department manager and an on-site visit. We use the security ontology as the basis for the inventory phase. The security ontology already contains knowledge regarding vulnerabilities, threats that exploit those vulnerabilities, and controls to mitigate them. Furthermore, the ontology contains an asset categorization skeleton that is used to model the organization-specific environment, e.g., existing control implementations and relevant business assets.

Figure 8 shows the basic layout of one floor level in Company A that we modeled ontologically in the inventory phase.

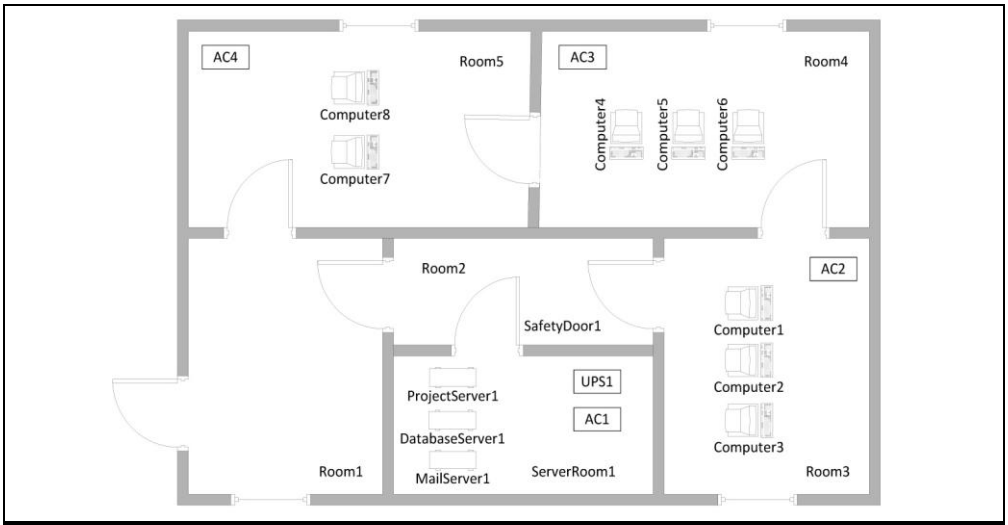

Figure 8. Floor Plan of Company A

The security ontology offers asset concepts such as Building, Level, Computer, Door, etc., with which the target environment can be mapped. Table 2 shows an excerpt of the gathered data including assets and their concept types.

Table 2: Input Data for the Ontology

Number	Department/Focus
ent:Organization	CompanyA
ent:Site	MainSite
ent:Building	MainBuilding
ent:Level	Level2
ent:Section	ServerRoom1
ent:Server	ProjectServer1
ent:Data	ProjectData

While ontology editors such as Protege[2] can be used for data entry, we developed a specialized risk management application[3] for our purposes, which directly accesses the underlying OWL ontology. Figure 9 shows the basic structure created with our application. Furthermore, it illustrates how assets can be added to the existing model. Right-clicking a node brings up the context menu, which offers to add resources depending on the ontology restrictions (e.g., allowed child elements of a Building are restricted to Levels). In this phase, all risk levels are set to zero, since impact levels as well as threat probabilities are still missing. Listing 1 shows a snippet of the standard underlying OWL RDF/XML representation of the generated data.

The relevant organizational environment (e.g., already existing control implementations) is inventoried in the same way and serves as basis for the further steps of our approach. Due to the multi-criteria nature of our approach, we

[2] Protege: http://protege.stanford.edu.
[3] Details on the risk management application AURUM (AUtomated Risk and Utility Management) are available at http://securityontology.sba-research.org/aurum/.

Listing 1: RDF/XML Source Code after the Initial Inventory

```
<Level rdf:ID="Level2">
        <asset_contains_Asset rdf:resource="#Room1"/>
        <asset_contains_Asset rdf:resource="#Room2"/>
        <asset_contains_Asset rdf:resource="#Room3"/>
        <asset_contains_Asset rdf:resource="#Room4"/>
        <asset_contains_Asset rdf:resource="#Room5"/>
        <asset_contains_Asset rdf:resource="#ServerRoom1"/>
        <asset_locatedIn_Asset rdf:resource="#MainBuilding"/>
        <rdfs:label xml:lang="en">Level 2</rdfs:label>
</Level>

<SafetyDoorA rdf:ID="SafetyDoorA_1">
        <sectionConnector_connects_Section rdf:resource="#Room2"/>
        <sectionConnector_connects_Section rdf:resource="#ServerRoom1"/>
</SafetyDoorA>

<Computer rdf:ID="DatabaseServer1">
        <asset_contains_Asset rdf:resource="#ClientData"/>
        <asset_contains_Asset rdf:resource="#FinancialData"/>
        <asset_contains_Asset rdf:resource="#ProjectData"/>
        <asset_locatedIn_Asset rdf:resource="#ServerRoom1"/>
        <rdfs:label xml:lang="en">DatabaseServer 1</rdfs:label>
</Computer>
```

require a set of criteria that describes potential control implementations and is in line with the strategic objectives of the company. The primary goal of both corporations is to implement security solutions that cover the need for protection optimally and are cost-efficient. Therefore, we included financial criteria and security-related objectives based on literature [cf. Avizienis et al., 2004] in the criteria set.

These criteria are merely a representative selection and can be adapted by the decision makers to the specific decision scenario (e.g., in order to take into consideration business partnerships or legal agreements). Note that different scales are applied depending on whether criteria can be measured in "real units" (e.g., monetary units, time units or measurable resource consumption) or not. If a category can be measured using a discrete number that relates to a real unit, candidates are assigned their absolute value. Otherwise (i.e., in case of intangible objectives such as Reliability), an abstract scale of levels such as low (L), medium (M), and high (H) is used. Additionally, each criterion is either of type benefit or of type resource, depending on whether the portfolios' category values should be maximized or minimized. An in-depth analysis led to the criteria set summarized below:

- Initial costs $q_{ic}(i)$ represent the amount of money an enterprise has to invest in order to integrate a countermeasure *i* into its corporate environment. This objective is of type "resource" and is measured using "monetary units" (MU).

- The term running costs $q_{rc}(i)$ should be self-explanatory. They either depend on the maintenance costs or the number of requests. This objective is of type "resource" and is measured in "monetary units" (MU).

- Effectiveness [cf. BJA, 2008] is defined as the ability to achieve stated goals or objectives, judged in terms of both output and impact. Although our potential countermeasure implementations are not directly related to a specific threat (i.e., defined goals or objectives are missing), their effectiveness can be rated based on their primary purpose. For example, the main purpose of a fire detector is to detect fire, and so we rate its effectiveness based on its ability to detect fire. At the current stage of research we are not considering side-effects of countermeasures (e.g., a security guard's primary purpose is to prevent unauthorized access but he would also be able to detect fire). This objective is of type "benefit" and is measured using levels L, M, and H.

- Reliability is defined by IEEE as the ability of a system or component to perform its required functions under stated conditions for a specified period of time (from *0* up to *t*). The distribution function $R(t)=1-F(t)$ defines the time to the first malfunction, $F(t)=exp(-t/T)$ is the case of an exponentially distributed time to malfunction, where parameter T defines the mean time to malfunction. This objective is of type "benefit" and is measured using levels L, M, and H.

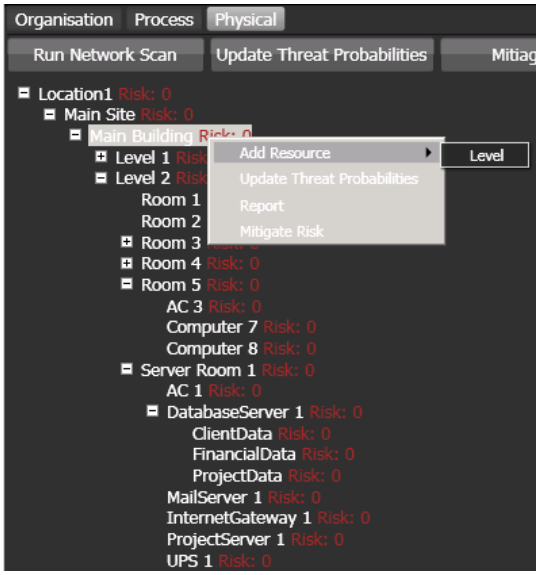

Figure 9. Inventory Company A

In the inventory phase we already saw examples of control implementations: e.g., the asset UPS1 represents an uninterruptible power supply unit in the server room. More specifically, an uninterruptible power supply unit of high effectiveness was installed. The criteria shown in Table 3 were defined for this asset type. The reader should note that information about controls has to be defined only once (along with threats, vulnerabilities, and control definitions) and can be reused by all organizations conducting a risk analysis with this framework.

Table 3: Uninterruptible Power Supply Unit Criteria

Name	Initial Costs	Running Costs	Effectiveness	Reliability
UninterruptiblePowerSupplyUnitC	1500	100	H	M

Because there is a control (UninterruptiblePowerSupplyControlCompliantSite) that requires the implementation of a power supply unit, this control will automatically be classified as compliant. Finally, other existing security control implementations, such as password policies and intrusion detection systems, were added according to the information from the IS department. At the end of the Inventory phase, we have an ontological model including all relevant assets of the organization.

Business Process Importance Determination

In the next step, Business Process Importance Determination (cf. Section Business Process Importance Determination), we focus on calculating availability importance values for relevant assets. To this end, we identified the primary business processes and received ADONIS process models which can be imported by our analysis tool. Details of an example process are shown in Figure 11.

Table 4: Business Process Importance Determination Example

Asset	Local (BP) Importance
ClientData	5000 Euro per hour
ProjectData	2500 Euro per hour
FinancialData	2500 Euro per hour
Computer1	5000 Euro per hour
ProjectServer1	5000 Euro per hour

Comparing the process description (cf. Figure 11) with the data collected in the inventory step (cf. Figure 9 and Listing 1), we can see that resources used in the workflow are already recorded in the ontological knowledge base (e.g., FinancialData and ProjectServer1). First, an importance value (either monetary or qualitative) has to be assigned to each business process. Based on this, resource importance values (focusing on availability) are calculated for each connected asset. In our example, the business process was assigned a value of 5,000 Euro per hour by the business process owner. After importing the example business process, the Availability Levels are determined automatically. Those values are stored in the ontological knowledge base along with the already

gathered data. When additional processes are imported, the importance values of the assets are aggregated if they are used in multiple processes. After all business processes have been imported, the business process owners review the importance values. They have the possibility to adjust the values based on their knowledge and to assign importance values to assets that were not connected in any business process definition. Figure 11 shows the details for the asset Project Data.

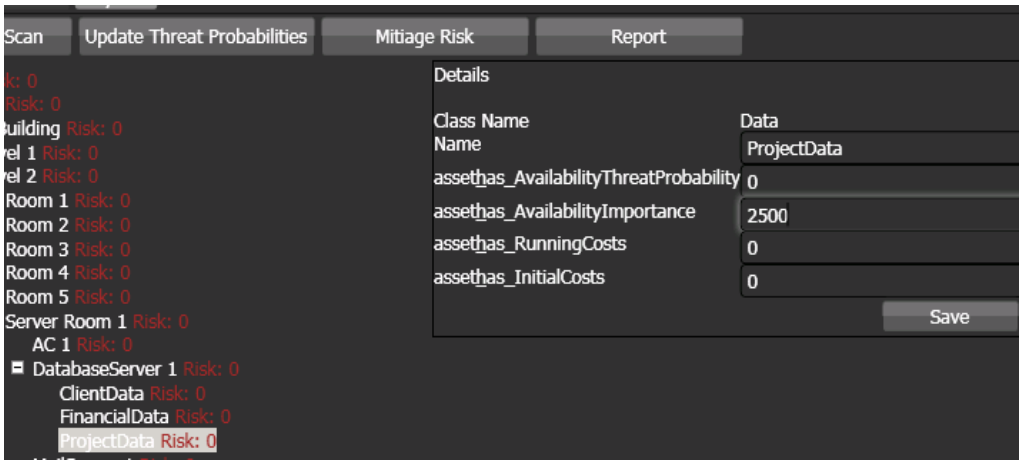

Figure 10. Project Data Importance Level

Company B, however, did not have business process models, so the Availability Levels could not be automatically determined. Instead, the values had to be entered manually by the process owners. Before threat probabilities can be calculated we need input values on attacker motivation and capability. We estimated this data together with the management. For company A the motivation was rated as medium on a three point scale, and the capability as high. These facts are also stored in the ontology. Please note that the ontological mapping of the organizational environment is the only input the decision maker has to provide for using this information security risk management approach. Further necessary knowledge regarding threats, vulnerabilities, and controls is provided by the security ontology.

Threat Probability Determination

After all the required data was entered and modeled in the ontology, we initiated the threat probability determination calculation as explained in Section Threat Probability Determination. To understand how the probability value is calculated, we have to consider existing threats, possible vulnerabilities, and the implemented controls. The probability calculation is demonstrated using the example of the threat Data Loss. Using our predefined knowledge base on threats, vulnerabilities, and controls, we find all threats that affect the availability of Data assets. In addition, threats against connected assets are also taken into consideration. E.g., Project Data is stored on the DatabaseServer1, so threats against computers are considered as well. Likewise, the server is located in the Main Building, so threats against the building are included in the probability calculation. Figure 12 shows a snippet of the Bayesian network used to calculate threat probabilities based on the organizational setting. The fact that a data backup policy is in place is derived from the ontological knowledge base and entered into the Bayesian network derived from the security ontology. The existence of this data backup policy makes the organization compliant with the 'Data Backup Strategy Control' and, as a result, closes the vulnerability 'No or Insufficient Data Backups'. The status of this vulnerability, along with other vulnerabilities and predecessor threats, influences the final Data Loss threat probability. To finally determine the data loss probability, our system uses reasoning engines to find all ontologically modeled countermeasures that implement one or more of the control specifications. The existence and effectiveness of each detected countermeasure is entered into the Bayesian network. E.g., an air conditioning system with low effectiveness is detected, and its effectiveness (0.3) is entered into the corresponding Bayesian network node. For 'Project Data' the following control implementations were detected, lowering the threat probability to 52 percent.

Risk Determination

The Risk Determination phase calculates threat probability values for business-relevant assets, which are multiplied by the impact values gained in the Business Process Importance Determination phase. Taking the detected control implementations into account, the data loss probability for the project data is 52 percent and the overall risk for

Communications of the Association for Information Systems

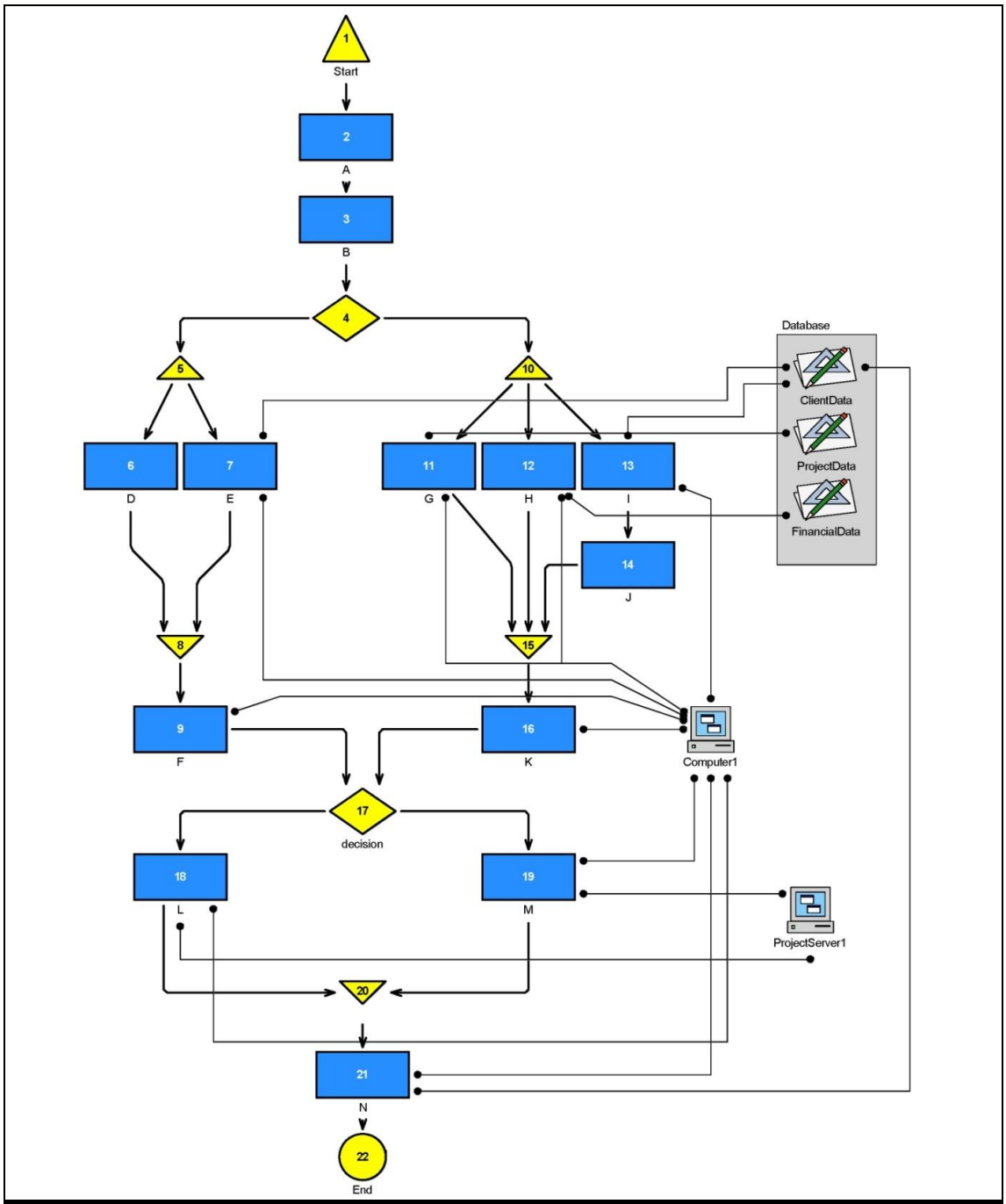

Figure 11. Business Process Company A

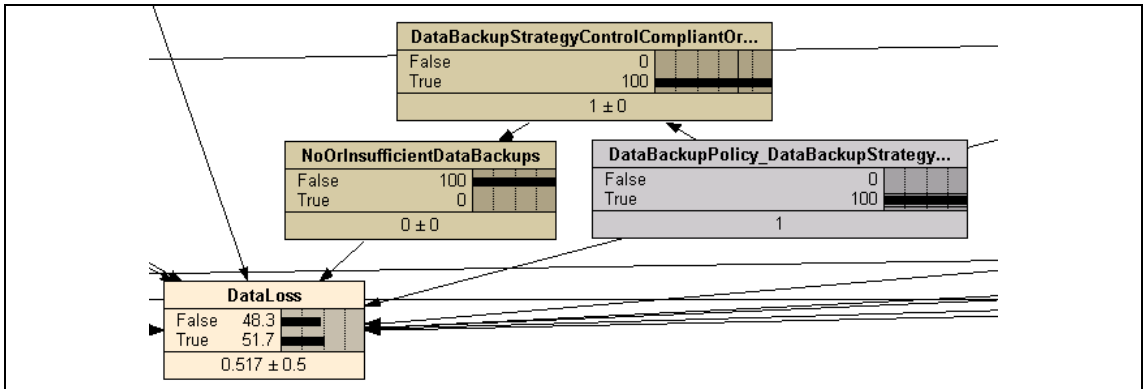

Figure 12. Data Loss Probability Calculation - Bayesian Network Snippet

Listing 2: Detected Control Implementations

```
Entering 0.3 and 0.7 at UninterruptiblePowerSupplyUnit_UninterruptiblePowerSupplyControlCompliantSite
Entering 0.3 and 0.7 at AirConditionSystem_AirConditioningInServerRoomControlCompliantServerRoom
Entering 1.0 and 0.0 at DataBackupPolicy_DataBackupStrategyControlCompliantOrganization
Entering 1.0 and 0.0 at DatabaseBackupPolicy_DatabaseBackupControlCompliantOrganization
Entering 1.0 and 0.0 at DatabasePermissionSettingPolicy_DatabasePermissionSettingControlCompliantOrg...
Entering 1.0 and 0.0 at DocumentationOfRoomMaintenancePolicy_DocumentationOfRoomMaintenanceControl...
Entering 1.0 and 0.0 at EscortationAndDocumentationOfAllVisitorsToServerRoom_EscortationAndDocumentation...
Entering 1.0 and 0.0 at ITTrainingOfAdministratorsPolicy_ITTrainingOfAdministratorsControlCompliant...
Entering 1.0 and 0.0 at RestrictionsOnAccessToServersPolicy_RestrictionsOnAccessToServersControl...
Entering 1.0 and 0.0 at StrongPasswordPolicy_StrongPasswordControlCompliantOrganization
Entering 1.0 and 0.0 at TestingOfFireExtinguishersPolicy_TestingOfFireExtinguishersControlCompliant...
Entering 1.0 and 0.0 at TestingOfStandbyGeneratorsPolicy_TestingOfStandbyGeneratorsControlCompliant...
Entering 1.0 and 0.0 at TrainingOfMaintenanceAndAdministrationStaffPolicy_TrainingOfMaintenanceAnd...
Entering 1.0 and 0.0 at UseOfKensingtonLocksPolicy_UseOfKensingtonLocksControlCompliantOrganization
Belief for DataLoss in the context of ProjectData: 0.5170552
```

Project Data amounts to 1,300 Euro per hour (2,500 Euro per hour * 0.52). This is the risk figure as described in Section Risk Determination. The risk figure is also calculated for all other business-relevant assets, such as data and IT systems. The result of the Risk Determination phase is a risk value assigned to each of these assets.

Control Identification and Evaluation

Prior to evaluating security solutions portfolios (cf. Section Control Identification and Evaluation) that can be used to lower the project data risk, a set of feasible candidates was automatically selected from the knowledge base. This selection was conducted by considering existing countermeasures and making a rough selection of potential candidates. The program compared their main characteristics with the decision situation's baseline parameters (exclusion criteria), such as available monetary or performance parameters. The number of candidates to include for individual evaluation strongly depends on several factors, including application domain and dependencies among the candidates, In this specific case, thirty-two candidates were selected. As an example, Table 5 shows candidates for the anti virus system group.

Table 5: Anti Virus System Group

Name	Initial Costs	Running Costs	Effectiveness	Reliability
Anti Virus System A	34	0	L	M
Anti Virus System B	29	7	H	H
Anti Virus System C	24	0	L	M

Some (combinations of) decision alternatives entail dependencies. For example, the ontological database states that the Access Regulation Control is fulfilled if either one or more Entry Checkpoints OR one or more Access Systems are deployed in security-sensitive sections. Other controls, such as the data backup control, require the organization to have a data backup policy AND a data backup server in place. Following the multi-objective decision support procedure, the process starts by evaluating the potential controls in combination with the dependencies taken from the ontology. In this way, 470 non-dominated (i.e., Pareto-efficient) feasible portfolios were identified for the company. These solution alternatives were then evaluated further using the interactive decision support module.

Figure 13 shows the initial screen of the analysis tool. By moving the red lines at the top and the bottom, aspiration levels are set (for minimum or maximum values in a given objective category), which reduces the number of remaining solutions in a straightforward manner. In our case studies, this was performed as follows: First, the maximum initial costs were lowered to a value of 12k, which reduced the number of portfolios from 450 to 290 (cf. Figure 14). After this, the minimum requirement for effectiveness was set to a level between medium and high, while the corresponding value for reliability was set to high. Afterwards, the remaining five sets of security solutions were visualized side by side (cf. Figure 15). The remaining portfolios (cf. Table 6) have the same reliability values, but differ in effectiveness values, initial costs, and running costs. Although solutions 2 and 4 have the highest effectiveness values, their initial and running costs are on the low and average side. With solution 3 the organization would get a solution that has a low effectiveness but is expensive (in terms of running costs). If we consider all potential portfolios in Case Study 1, the remaining portfolios provide high benefits (effectiveness and reliability) and require average resources (initial and running costs).

Note that the control implementations contained in the remaining portfolios as well as their values are on a similar level due to the restrictions made by the decision maker. Depending on the decision maker's preferences, they can either select one of these or continue the evaluation process by picking other portfolios and/or (re-)setting the aspiration levels. In comparison to Company A, Company B had more security control implementations already in place. For example, an Entry Checkpoint existed, Anti Virus Systems were enforced company wide and a Locked Doors Policy was in place. As a result, the number of control implementation candidates and the overall portfolio costs were substantially lower.

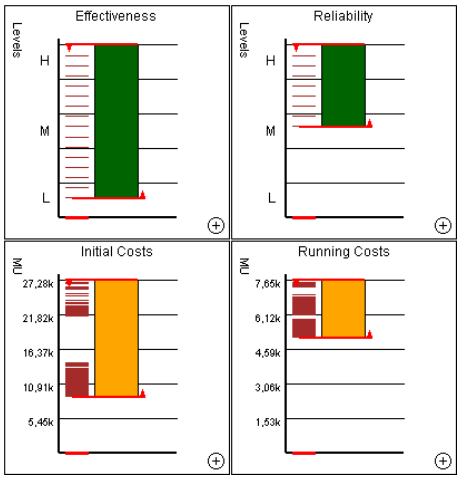

Figure 13. Initial Mask

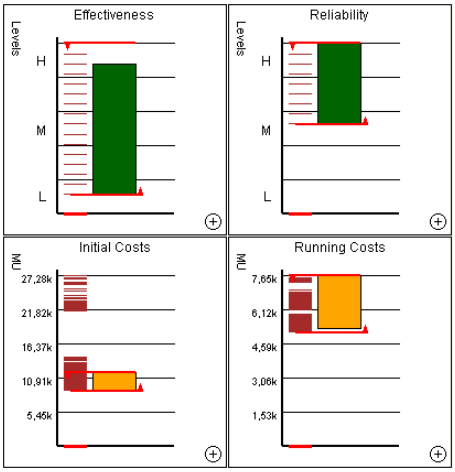

Figure 14. Mask After the User's First Setting

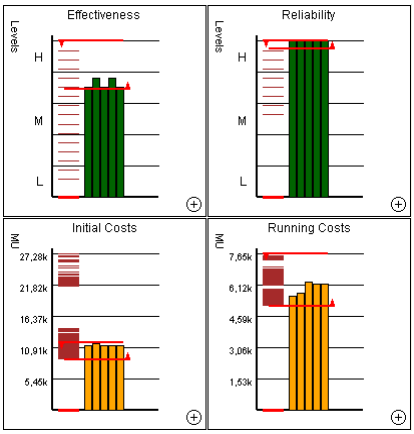

Figure 15. Mask After the User's Second Setting

Table 6: List of the Remaining Portfolios[4]					
Set	**Name**	**Initial Costs**	**Running Costs**	**Effectiveness**	**Reliability**
1	AVS B, LDP B, AS A, HD C, DD C, DBD B, SD C, DBP B	12	17	11405	5618
2	AVS B, LDP B, AS A, HD C, DD C, DBD B, SD B, DBP B	13	17	11675	5757
3	AVS B, LDP B, AS C, HD C, DD C, DBDB, SD A, DBP A	12	17	11295	6278
4	AVS B, LDP B, AS A, HD C, DD C, DBD B, SD A, DBP A	13	17	11425	6225
5	AVS B, LDP B, AS A, HD C, DD A, DBD B, SD A, DBP A	12	17	11282	6225

From the calculated portfolios (cf. Table 6), company A decided to implement Solution 2 due to its high effectiveness and lower running costs. As shown in Table 1, the selection of the preferred portfolio completes the cycle and feedback begins. To see the effects of the portfolio, we start again with the Inventory phase. New assets from the chosen portfolio, such as the Anti Virus System, a Data Disposal policy, and the Access System, are added to our existing model. After modeling these assets, we can initiate a recalculation of the threat probabilities. The new probability values take the newly implemented security controls into account and reflect the changes resulting from the portfolio implementation. Looking back at the previous example of Data Loss, a new threat probability of 32 percent is calculated for Project Data. The overall risk for Project Data now amounts to 800 Euro per hour (2,500 Euro per hour * 0.32). In exactly the same manner we can test the risk implications of the remaining portfolios. Management at Company A decided to accept the data loss risk for the Project Data. They are planning to decrease the risk level further as soon as a new security budget becomes available.

Listing 3: Detected Control Implementations

```
Entering 1.0 and 0.0 at ObjectUnionOf(AccessSystem EntryCheckpoint)_AccessRegulationControlCompliantSection
Entering 0.5 and 0.5 at TransactionSecurityAndVirusProtectionSoftware_UseOfAntivirusSoftwareControl...
Entering 0.3 and 0.7 at UninterruptiblePowerSupplyUnit_UninterruptiblePowerSupplyControlCompliantSite
Entering 0.3 and 0.7 at AirConditionSystem_AirConditioningInServerRoomControlCompliantServerRoom
Entering 0.3 and 0.7 at HeatDetector_HeatDetectorInServerRoomControlCompliantServerRoom
Entering 1.0 and 0.0 at DataBackupMediaLabelingPolicy_BackupProcedureDocumentationControl...
Entering 1.0 and 0.0 at DataBackupProcedureDocumentationPolicy_BackupProcedureDocumentationControl...
Entering 1.0 and 0.0 at CloseDoorsAndWindowsAfterWorkingHoursPolicy_ClosedDoorsAndWindowsControl...
Entering 1.0 and 0.0 at DataBackupPolicy_DataBackupStrategyControlCompliantOrganization
Entering 1.0 and 0.0 at DatabaseBackupPolicy_DatabaseBackupControlCompliantOrganization
Entering 1.0 and 0.0 at DatabasePermissionSettingPolicy_DatabasePermissionSettingControlCompliant...
Entering 1.0 and 0.0 at DocumentationOfRoomMaintenancePolicy_DocumentationOfRoomMaintenance...
Entering 1.0 and 0.0 at EscortationAndDocumentationOfAllVisitorsToServerRoom_EscortationAndDocumentation...
Entering 1.0 and 0.0 at ITTrainingOfAdministratorsPolicy_ITTrainingOfAdministratorsControlCompliant...
Entering 1.0 and 0.0 at DataBackupMediaAccessStrictlyRestrictedPolicy_RestrictAccessToBackupMediaControl...
Entering 1.0 and 0.0 at RestrictionsOnAccessToAccountsOrTerminalsPolicy_RestrictionsOnAccessToAccounts...
Entering 1.0 and 0.0 at UseOfScreenLockPolicy_RestrictionsOnAccessToAccountsOrTerminalsControlCompliant...
Entering 1.0 and 0.0 at RestrictionsOnAccessToServersPolicy_RestrictionsOnAccessToServersControlComplian...
Entering 1.0 and 0.0 at SecureDispositionOfMediaPolicy_SecureDispositionOfMediaControlCompliantOrganization
Entering 1.0 and 0.0 at StrongPasswordPolicy_StrongPasswordControlCompliantOrganization
Entering 1.0 and 0.0 at TestingOfFireExtinguishersPolicy_TestingOfFireExtinguishersControlCompliant...
Entering 1.0 and 0.0 at TestingOfStandbyGeneratorsPolicy_TestingOfStandbyGeneratorsControlCompliant...
Entering 1.0 and 0.0 at TrainingOfMaintenanceAndAdministrationStaffPolicy_TrainingOfMaintenanceAnd...
Entering 1.0 and 0.0 at UseOfKensingtonLocksPolicy_UseOfKensingtonLocksControlCompliantOrganization
Belief for DataLoss in the context of ProjectData: 0.32025476
```

V. VALIDATION

The case studies gave us the following insights regarding the initial research questions:

- RQ1: How can we comprehensibly calculate information security standard-compliant IT security solution portfolios?

Comprehensibility was a key element in the design and implementation of AURUM. User feedback from the conducted case studies showed that users benefit from the highly automated but still comprehensible AURUM methodology (especially in nontechnical environments such as the Finance and Controlling department in Case Study 1). The interactive security control implementation selection enabled even nontechnical users such as management to assess how the implementation of certain controls influences the final risk level regarding specific assets. Our decision support system allows them to choose security solution portfolios based on their preferences regarding the criteria initial costs, running costs, effectiveness, and reliability. Our formal and comprehensive information security knowledge base (security ontology) enabled organizations in both case studies to leverage the

[4] Anti Virus System (AVS), Locked Doors Policy (LDP), Access System (AS), Heat Detector (HD), Data Disposal (DD), Data Backup Documentation (DBD), Safety Door (SD), Data Backup Policy (DBP)

formal threat, vulnerability, and control knowledge to efficiently minimize risk levels of their business-critical assets. Both organizations estimated the time necessary to initially assess potential threats, vulnerabilities, and controls without this formal knowledge base and the corresponding AURUM tool to about three working days (based on their previous risk management activities that were supported by handmade spreadsheets and information security best practice guidelines). With the formal knowledge base and the developed tools at hand, the organizations only had to model their infrastructure within the framework. Relevant threats, vulnerabilities, and control implementations were determined automatically by AURUM. By using the AURUM approach the time required for conducting all risk management phases (as shown in Figure 1) was reduced to one working day in Company A and one and a half working days in Company B. In our case studies we considered thirty-one threats and ninety-two corresponding vulnerabilities in both organizations. In Company A we identified nineteen threats and fifty-three vulnerabilities that had not been considered in their previous risk management activities. In Company B we identified eleven such threats and twenty-three vulnerabilities. Because of the vulnerabilities that were not considered in the companies' previous risk management activities, AURUM suggested fifty-seven additional control implementations in Company A and twenty-six additional control implementations in Company B. Please note that some vulnerabilities required more than one control implementation for mitigation.

While in previous risk assessments the importance determination relied on the intuition of the process owners and managers, our approach calculated the impact values of resources based on business process involvement in Company A. In general, the automated importance determination approach generated consistent importance values for involved resources and, therefore, delivered a consistent basis for the subsequent risk determination. Based on their experience and previous risk assessments, process owners at both companies mostly agreed with the importance values given by AURUM. For resources that had not been fully considered in previous risk management activities (e.g., power lines), process owners first disagreed on the calculated importance value. After explaining the relevant dependencies (e.g., that the project server relies on a working power line), the process owners accepted and agreed on these importance values. In the probability determination phase, Company A had estimated the threat probabilities qualitatively (on a three-point scale from high to low) in previous risk assessments. By using the proposed Bayesian network approach, we were able to gain consistent probability values that took all vulnerabilities and existing control implementations into account. Furthermore, the calculated probability percentages allowed for a more differentiated risk estimation than qualitative ratings and provided both companies with comprehensible probability figures.

By means of the formal relationships in the security knowledge base, controls were automatically recommended based on the identified threats and vulnerabilities. Compared to the companies' previous risk management activities, AURUM provided efficient control implementation portfolios that took the organization-specific threat landscape of both companies into account. As the main goal of risk management is to assess and reduce risk to an acceptable level, an expert panel evaluated the threats, vulnerabilities, control implementation suggestions, and risk figures considered and calculated by AURUM in both companies. Each of the three expert panel members has worked in the information security domain with a focus on risk management for more than five years. The expert panel confirmed that AURUM considered important threats and vulnerabilities missing in previous risk management activities. As a result, AURUM provided both companies with additional control implementations to mitigate the newly discovered vulnerabilities (fifty-seven additional control implementations in Company A and twenty-six in Company B). As these vulnerabilities were not considered in the companies' previous risk management activities, the expert panel confirmed that AURUM suggested reasonable control implementation portfolios to reduce the risk to the companies' resources. The recommended control implementations together with the portfolio selection approach allow decision makers to select the optimal solution in terms of efficiency, reliability, and budget restrictions. Thus, AURUM eliminated the false sense of security generated by the companies' previous risk management activities and reduced the risks to their resources by suggesting appropriate control implementation portfolios that take the organization-specific security settings into account.

- RQ2: How can we effectively communicate the portfolios' risk versus cost trade-off figures to management decision makers?

The developed interactive decision support system and the corresponding data gathering and risk calculation techniques helped management decision makers in the conducted case studies to understand the risk versus cost trade-offs during the control selection and evaluation. In both case studies, decision makers appreciated the immediate feedback regarding potential security solution portfolios when (re-)setting the aspiration levels of our four benefit and resource categories. The abstract view allowed them to focus only on the resource and benefit categories without having to consider technical details of the solutions.

In response to our initial problem statement, we validated the developed AURUM methodology and its tool implementation by comparing its functionality to existing methodologies and their tool implementations: GSTool

(described in [BSI, 2004]) and CRISAM (described in [Stallinger, 2007]). Table 7 shows the results of the comparison.

Table 7: AURUM, GSTool, CRISAM Comparison

Issue	AURUM	GSTool	CRISAM
Domain expert dependence	yes	yes	yes
Automated threat–infrastructure mapping	yes	no	no
Concrete implementation suggestions	yes	no	no
Comprehensible threat probability determination	yes	no	no
Measurable IT security solution effectiveness	yes	no	no
Interactive decision support	yes	no	no

Although AURUM was designed to minimize domain expert dependence, the case studies showed that domain experts still have to be consulted in the inventory and control implementation phases. However, the high degree of automation in the remaining phases and the interactive security solution portfolio selection supported inexperienced users (e.g., process owners) in choosing security solutions for "their" domain. GSTool and CRISAM do not show explicitly which threats endanger the modeled infrastructure and do not calculate threat probabilities. Because of the underlying ontological knowledge model, AURUM determines which threats are relevant to each component of the modeled infrastructure based on asset classes. By using the formal knowledge base, reasoning engines, and Bayesian networks, the threat probability is determined in a mathematically sound and comprehensible way. The case studies showed that the automated and comprehensible AURUM workflow helped users to focus on the most relevant tasks in risk management: providing appropriate input data and selecting security solution portfolios based on organization-specific constraints. When it comes to control selection, CRISAM and GSTool lack required functionality and user support. AURUM provides users with concrete implementation suggestions and calculates potential security solution portfolios based on constraints that are defined interactively by the user.

VI. CONCLUSION

Companies consider security one of the most important issues on their agenda, because the increasing number of security breaches poses a major threat to the reliable execution of corporate strategies and can have negative effects on business value. Information security risk management ensures that all possible threats and vulnerabilities, as well as the valuable assets, are taken into consideration. Existing approaches, such as best practice guidelines, information security standards, or domain experts, but also information security risk management approaches that are highly accepted within the community all have shortcomings.

This article presented a methodology for supporting a typical information security risk management process (such as NIST SP 800-30). We implemented this approach in a tool and tested it in two case studies. The results of the case studies showed that this methodology provides the following benefits compared to existing approaches: (1) the ontological information security knowledge base ensures that the information security knowledge is provided to the risk manager in a consistent and comprehensive way, (2) modeling the organization's assets within our ontological framework ensures that assets are modeled in a consistent way, (3) the incorporation of existing best practice guidelines and information security standards ensures that only widely accepted information security knowledge is used for threat/vulnerability identification and control recommendations, (4) the proposed Bayesian threat probability determination ensures that the threat probability determination has a more objective basis than existing approaches, (5) threat impacts can be automatically calculated after the initial rating of assets, (6) controls to reduce risks to an acceptable level are offered automatically, (7) the use of interactive decision support allows decision makers (e.g., the risk manager) to investigate various scenarios and, as a result, to learn more about the characteristics of the underlying problem, while the system guarantees that only an efficient solution can be selected, and (8) by considering multiple objectives and providing gap analysis we support decision makers in getting a much better understanding of the problem in terms of what can be achieved in some objectives at what "price" in terms of opportunity costs in other objectives.

ACKNOWLEDGMENTS

This work was partly performed at the research center SBA Research funded by the Federal Ministry of Economy, Family and Youth of the Republic of Austria, and by the City of Vienna.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Aime, M., A. Atzeni, and P. Pomi (2007) "AMBRA: Automated Model-Based Risk Analysis",*Proceedings of the 2007 ACM Workshop on Quality of Protection* (QoP '07), New York, NY: ACM, pp. 43–48.

Alberts, C. et al. (2003) *Introduction to the OCTAVE Approach*, Technical Report, Pittsburgh, PA: Carnegie Mellon—Software Engineering Institute.

Arora, A. et al. (2004) "Measuring the Risk-Based Value of It Security Solutions", *IT Pro* (6), pp. 35–42.

Avizienis, A. et al. (2004) "Basic Concepts and Taxonomy of Dependable and Secure Computing", *IEEE Transactions on Dependable and Secure Computing* (1), pp. 11–33.

Bagchi, K. and G. Udo (2003) "An Analysis of the Growth of Computer and Internet Security Breaches", *Communications of the Association for Information Systems* (12), pp. 684–700.

Baker, W., L. Rees, and P. Tippett (2007) "Necessary Measures: Metric-Driven Information Security Risk Assessment and Decision Making", *Communications of the ACM* (50), pp. 101–106.

Baker, W. and L. Wallace (2007) "Is Information Security under Control? Investigating Quality in Information Security Management", *IEEE Security and Privacy* (5), Piscataway, NJ: IEEE Educational Activities Department, pp. 36–44.

Bandyopadhyay, K. and P. Mykytyn (1999) "A Framework for Integrated Risk Management in Information Technology", *Management Decision* (37), pp. 437–444.

Baskerville, R. (1993) "Information Systems Security Design Methods: Implications for Information Systems Development", *ACM Computing Surveys* (25), pp. 375–414.

BERR (2008) *2008 Information Security Breaches Survey*, Technical Report, Department for Business Enterprise and Regulatory Reform.

BJA, B. (2008) "Center for Program Evaluation—Glossary", http://www.ojp.usdoj.gov/BJA/evaluation/glossary/ (current Jan. 30, 2011).

Bodin, L., L. Gordon, and M. Loeb (2008) "Information Security and Risk Management", *Communications of the ACM* (51), pp. 64–68.

BSI (2004) "IT Grundschutz Manual", https://www.bsi.bund.de/ContentBSI/grundschutz/grundschutz.html (current Jan. 30, 2011).

Burtles, J. (2007) *Principles and Practice of Business Continuity: Tools and Techniques*, Brookfield, CT: Rothstein Associates, Inc.

Cavusoglu, H., B. Mishra, and S. Raghunathan (2004a) "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", *International Journal of Electronic Commerce* (9), pp. 69–104.

Cavusoglu, H., B. Mishra, and S. Raghunathan (2004b) "A Model for Evaluating IT Security Investments", *Communications of the ACM* (47), pp. 87–92.

Commission of the European Communities (2006) *Communication from the Commission to the Council, The European Parliament, The European Economic and Social Committee and the Committee of the Regions: A Strategy for a Secure Information Society—Dialogue, Partnership and Empowerment* (COM 2006), 251 final.

DCSSI (2004) *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)—Section 2—Approach*, General Secretariat of National Defence Central Information Systems Security Division (DCSSI).

ENISA (2006) *Risk Management: Implementation Principles and Inventories for Risk Management/Risk Assessment Methods and Tools*, Technical Report, European Network and Information Security Agency.

Farquhar, B. (1991) “One Approach to Risk Assessment”, *Computers and Security* (10), pp. 21–23.

Fenz, S. and A. Ekelhart (2009) “Formalizing Information Security Knowledge”, *Proceedings of the 4th ACM Symposium on Information, Computer, and Communications Security*, pp. 183–194.

Fenz, S., A. Ekelhart, and T. Neubauer (2009) “Business Process-Based Resource Importance Determination”, *Proceedings of the 7th International Conference on Business Process Management* (BPM 2009), Springer Berlin Heidelberg, Lecture Notes in Computer Science, Vol. 5701, pp. 113–127.

Fenz, S. and T. Neubauer (2009) “How to Determine Threat Probabilities Using Ontologies and Bayesian Networks”, *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research* (CSIIRW '09), ACM.

Fenz, S., A. Tjoa, and M. Hudec (2009) “Ontology-Based Generation of Bayesian Networks”, *International Conference on Complex, Intelligent and Software Intensive Systems* (CISIS '09), IEEE Computer Society, pp. 712–717.

Finne, T. (1998a) “A Conceptual Framework for Information Security Management”, *Computers & Security* (17), pp. 303–307.

Finne, T. (1998b) “The Three Categories of Decision-Making and Information Security”, *Computers & Security* (17), pp. 397–405.

FIPS (1975) *Guideline for Automatic Data Processing Risk Analysis*, Federal Information Processing Standards Publications (FIPS PUB) 65, National Bureau of Standards.

Fredriksen, R. et al. (2002) “The Coras Framework for a Model-Based Risk Management Process”, *SAFECOMP'02: Proceedings of the 21st International Conference on Computer Safety, Reliability and Security*, London, England: Springer-Verlag, pp. 94–105.

Frosdick, S. (1997) “The Techniques of Risk Analysis Are Insufficient in Themselves”, *Disaster Prevention and Management* (6), pp. 165–177.

Gerber, M. and R. von Solms (2004) “Management of Risk in the Information Age”, *Computers & Security* (24), pp. 16–30.

Gómez-Pérez, A., M. Fernández-López, and O. Corcho (2004) *Ontological Engineering*, New York, NY: Springer Heidelberg.

Gordon, L. and M. Loeb (2002) “The Economics of Information Security Investment”, *ACM Transactions on Information and System Security* (5), pp. 438–457.

Herzog, A., N. Shahmehri, and C. Duma (2007) “An Ontology of Information Security”, *International Journal of Information Security and Privacy* (1), pp. 1–23.

ISO/IEC (2005) *ISO/IEC 27001:2005, Information Technology–Security–Techniques–Information Security Management Systems–Requirements*.

ISO/IEC (2007) *ISO/IEC 27005:2007, Information Technology–Security Techniques–Information Security Risk Management*.

Ittner, C.D. and D.F. Larcker (2003) “Coming Up Short on Nonfinancial Performance Measurement”, *Harvard Business Review* (81), Philadelphia, PA: Wharton School, University of Pennsylvania, http://view.ncbi.nlm.nih.gov/pubmed/14619154 (current Jan. 30, 2011).

Järvinen, P. (2000) “Research Questions Guiding Selection of an Appropriate Research Method”, *Proceedings of the 8th European Conference on Information Systems, Trends in Information and Communication Systems for the 21st Century* (ECIS 2000), Vienna, Austria, July 3–5, pp. 124–131.

Jung, C., I. Han, and B. Suh (1999) “Risk Analysis for Electronic Commerce Using Case-Based Reasoning”, *International Journal of Intelligent Systems in Accounting, Finance & Management* (8), pp. 61–73.

Kairab, S. and L. Kelly (2004) *A Practical Guide to Security Assessments*, Boston, MA: Auerbach Publications.

Kim, A., J. Luo, and M. Kang (2005) “Security Ontology for Annotating Resources”, *OTM Conferences* (2), pp. 1483–1499.

Lander, D.M. and G.E. Pinches (1998) “Challenges to the Practical Implementation of Modeling and Valuing Real Options”, *The Quarterly Review of Economics and Finance* (38), pp. 537–567, http://ideas.repec.org/a/eee/quaeco/v38y1998i3p537-567.html (current Jan. 30, 2011).

Neubauer, T. and C. Stummer (2007) “Extending Business Process Management to Determine Efficient IT Investments”, *Proceedings of the 2007 ACM Symposium on Applied Computing* (SAC '07), pp. 1250–1256.

NIST (1995) *An Introduction to Computer Security—The NIST Handbook*, Technical Report, NIST (National Institute of Standards and Technology), Special Publication 800-12, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (current Jan. 30, 2011).

Peltier, T.R. (2005) *Information Security Risk Analysis, 2nd edition*, Boston: Auerbach Publications.

PITAC (2005) *Cyber Security: A Crisis of Prioritization: Report to the President*, Technical Report, President's Information Technology Advisory Committee.

Rainer, R., C. Snyder, and H. Carr (1991) “Risk Analysis for Information Technology”, *Journal of Management Information Systems* (8), pp. 129–147.

Ryan, S.D. and M.S. Gates (2004) “Inclusion of Social Sub-System Issues in IT-Investment Decisions: An Empirical Assessment”, *Information Resources Management Journal* (17), pp. 1–18.

Sage, A. and E. White (1980) “Methodologies for Risk and Hazard Assessment: A Survey and Status Report”, *IEEE Transactions on Systems, Man, and Cybernetics* (SMC-10), pp. 425–446.

Schumacher, M. (2003) *Security Engineering with Patterns—Origins, Theoretical Model, and New Applications,* New York, NY: Springer.

Smith, S. and E. Spafford (2004) “Grand Challenges in Information Security: Process and Output”, *IEEE Security & Privacy* (2), pp. 69–71.

Soo Hoo, K. (2000) *How Much Is Enough? A Risk Management Approach to Computer Security*, Ph.D. Thesis, Stanford University.

Stallinger, M. (2007) *IT-Governance im Kontext Risikomanagement*, Ph.D. Thesis, Johannes Kepler Universität Linz.

Stoneburner, G., A. Goguen, and A. Feringa (2002) *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30, Gaithersburg, MD: National Institute of Standards and Technology (NIST).

Straub, D. and R. Welke (1998) “Coping with Systems Risk: Security Planning Models for Management Decision Making”, *MIS Quarterly* (22), pp. 441–469.

Vitale, M. (1986) “The Growing Risks of Information Systems Success”, *MIS Quarterly* (10), pp. 327–334.

W3C (2004) “OWL—Web Ontology Language”, http://www.w3.org/TR/owl-features/ (current Jan. 30, 2011).

ABOUT THE AUTHORS

Dr. Stefan Fenz is a senior researcher at Vienna University of Technology and SBA Research. In 2010 Stefan worked as a visiting scholar at Stanford Center for Biomedical Informatics Research at Stanford University. His primary research is on information security, with a secondary interest in semantic technologies and named entity recognition. Stefan received an MSc in software engineering and Internet computing from Vienna University of Technology, an MSc in political science from University of Vienna, an MSc in business informatics from Vienna University of Technology, and a Ph.D. in computer science from Vienna University of Technology. He is a member of the IFIP WG 11.1—Information Security Management, the IEEE Systems, Man, and Cybernetics Society and ISC2.

Andreas Ekelhart is a researcher and project manager at SBA Research. His research focuses mainly on applied concepts of IT security and semantic applications, on which he specialized during his studies. He received a Master's in Business Informatics from the Vienna University of Technology and a Master in Software Engineering & Internet Computing from the Vienna University of Technology. Currently he is working on his Ph.D. thesis at the Institute of Software Technology and Interactive Systems in cooperation with Secure Business Austria.

Dr. Thomas Neubauer is a senior researcher and project manager at the Institute of Software Technology and Interactive Systems (ISIS) at the Vienna University of Technology. His research focuses on the integration of security concepts into business process management, support for management decision makers in formulating a reasonable risk versus cost trade-off when investing in IT security solutions and measuring the actual level of security. Another research focus is the improvement of privacy enhancing technologies, especially in the field of e-health. He was granted a patent titled "Data Processing System for the Processing of Object Data" in September 2007. He has published over sixty papers in refereed journals and at international conferences. He worked in the financial sector for two years and as a consultant for the Austrian Federal Chancellery (CIO Office) and the Austrian Social Security Institutions.

Communications of the Association for Information Systems

ISSN: 1529-3181

Communications of the Association for Information Systems