FORISK: Formalizing Information Security Risk and Compliance Management

Stefan Fenz, Thomas Neubauer
Vienna University of Technology, Austria
{*stefan.fenz, thomas.neubauer*}@*tuwien.ac.at*

Rafael Accorsi, Thomas Koslowski
University of Freiburg, Germany
{*rafael.accorsi, thomas.koslowski*}@*iig.uni-freiburg.de*

***Abstract*—Regulatory frameworks and economic pressure demand decision makers to define mitigation strategies for their operational IT risks. However, recent studies indicate the lack of IS knowledge at the management level is one reason for inadequate or nonexistent IS risk management strategies because existing approaches fall short of meeting decision makers' needs. This paper presents the FORISK project that provides a new approach to support decision makers in interactively defining the optimal set of resilient measures and security controls according to regulations and standards. FORISK addresses three essential, yet unsolved research problems: (i) the formal representation of IS standards and domain knowledge, (ii) the reliable risk determination, (iii) and the (semi-)automated countermeasure definition.**

***Keywords*-semantic technolgies, compliance management, resilience management, information security;**

I. Introduction

The importance of information technology (IT) brought up the urgent need to ensure its continuous and reliable operation and to protect the processed and stored data. The intensive use of interconnected and complex IT-systems incurs risks with increasingly severe disruptive effects. As a consequence, managing evolving IT risks is imperative for modern organizations to ensure continuous and reliable operation and to protect the transmitted and stored data [1]. Common frameworks, such as the Sarbanes-Oxley act and Basel II/III, demand decision makers to define mitigation strategies for their operational IT risks.

However, since data protection, privacy regulations, and security standards are a complex range of requirements to which decision makers have to respond, organizations are increasingly forced to rethink how they perform risk and compliance management and, equally, how they address the security and resilience of their business processes. There is, thus, a pressing need for an overarching information security framework able to provide context and coherence to risk and compliance activities. To date, though, organizations have mostly relied on best practice guidelines, information security standards, or domain experts to conduct the risk assessment and mitigation phases. The prohibitive costs of such approaches can lead to the ignorance of risk assessment. In fact, according to the 2008 Information Security Breaches Survey [2], only 48% of 1,007 interviewed UK organizations formally assess information security risks. While approaches based on best practices, standards and experts can substantially support organizations in managing risks, they have a variety of shortcomings. In particular, because decision makers have to "manually" deal with the following key questions: (1) What are potential threats for my organization?; (2) What is the likelihood of these threats?; (3) What is the potential impact of a particular threat?; (4) Which vulnerabilities could be exploited by such threats?; (5) Which controls are required to mitigate these vulnerabilities?; and finally (6) What are the investments in security worth?

While in-depth knowledge of the organization in question and the IS domain as a whole is fundamental to existing approaches, little research has been conducted on the knowledge representation of the domains that are relevant to IS risk management. Recent studies indicate the lack of IS knowledge at the management level as one reason for inadequate or missing IS risk management strategies [3].

This paper gives an overview of the FORISK project which aims to provide decision makers with a fundamentally new approach for risk management incorporating resilience and compliance considerations. FORISK contributes to research in the areas of qualitative and quantitative information security risk and compliance management with an emphasis on decision support.

II. Research Questions and Objectives

A myriad of limitations with existing IS risk and resilience approaches such as exist:

- Best practice guidelines provide good information about potential threats, vulnerabilities, and controls, but without an information security domain expert, the organization is usually unable to consider the many complex relationships between all the relevant information security concepts, which results in a non-comprehensive information security approach that endangers the performance of the organization's mission.
- Information security standards, such as ISO 27001/27002, tend to state very abstract implementation suggestions for risk mitigation; concrete measures or combinations thereof are mostly missing, leading to inefficient or even misleading risk mitigation strategies. Effective tools that could be used for the automated compliance check are missing.

- In order to identify the concrete infrastructure elements at risk, the organization has to manually combine the knowledge from best practice guidelines with their actual infrastructure.
- The determination of threat probabilities is predominantly based on subjective perceptions and not on an objective evaluation.
- While companies strive for cost-conscious solutions, they are frequently unaware of their level of IT security capital expenditure or, even more importantly, whether these investments are effective.
- Management decision makers, such as the CPO or CIO, are faced with a great spectrum of potential IT security investments on the one hand and the decision of choosing the most appropriate set of IT security investments on the other hand. Existing methods provide decision makers with limited intuitive and interactive decision support and, thus, fail to support them in making an appropriate risk versus cost trade-off when deciding on the optimal level of investments in IT security solutions.

FORISK pursues to carve these essential yet open issues by providing a new approach to support decision makers in interactively defining the optimal set of security controls and resilience principles according to common regulations and standards. The proposed project involves three essential yet unsolved research problems:

RQ1: **Formal Information Security Standards Representation:** How can decision makers (and organizations) be supported in assessing, defining and selecting the optimal level of security investments (and thereby making an appropriate risk versus cost trade-off) in line with given business processes, multiple objectives such as acceptable risk level or resource constraints and interdependencies? And more precisely, how can they be supported in which ISO27002 controls is it worth/necessary investing?

RQ2: **Risk and Resilience Determination:** How can business processes be used to determine assets' importance (potential impact) in the overall organizational context? How can risk levels of business processes (i.e., the probability that the business process does not deliver the expected output) be determined based on assets' importance as well as implemented safeguards, applicable a priori probabilities, and relevant attacker profiles?

RQ3: **(Semi-) automated Countermeasure Definition:** What and how much data has to be presented for risk management and how must the data be displayed to decision makers in order to support them in making the optimal decision according to their corporate requirements?

In order to answer these research questions FORISK makes the following contributions:

(i) Support decision makers in focusing on the essential parts of the compliance check: defining risk mitigation strategies. The ontology developed brings the abstract suggestions stated in standards to a concrete level and extracts the information that is necessary for an effective and efficient decision. (ii) Provide decision makers with a methodology for defining countermeasures (and thereby making the appropriate risk versus cost trade-off) in an interactive and intuitive way while the system automatically ensures that the selected solution will be efficient with respect to given business processes, acceptable risk and resilience levels, and resource constraints. (iii) Make a major step beyond state of the art by introducing a methodology that allows a (semi-)automated compliance check based on the ISO27001/27002 standard. (iv) Render the tedious work of manually combing the knowledge from best practice guidelines with their actual infrastructure obsolete. (v) Allow the objective evaluation of risks in accordance with corporate business processes and the demand for protection instead of subjective perceptions. (vi) Provide decision makers with a framework characterized by ease of operation and efficient handling, such as decision makers are used to it, e.g., from using their iPad. The subjective user experience is an essential factor for the success of methodologies intend to be used by top management. Furthermore, usability allows cost reduction and faster project cycles due to a higher level of user acceptance and user satisfaction. (vii) Provide a formal and standardized representation of the ISO27002 standard within an ontology and thereby provide a "common language" in the area of risk management to facilitate communication of stakeholders. (viii) Enable an ex post assessment and control-loop of business process resilience based on exploratory mining techniques. (ix) Build the methodologies on the requirements made by top management decision makers and evaluates the applicability of the approaches in practice.

III. FORISK Framework

In this section we provide an overview of the FORISK framework. The main modules are illustrated in Figure 1.

A. Business Process Importance Determination

Based on business process models and an overall importance value for each business process, asset importance values are automatically calculated. As input we use business process models, such as provided by business process management solutions ARIS and ADONIS, including required assets connected on the activity level, which are internally transformed into Petri nets for further processing. In addition, for each business process an importance value is assigned, either monetary (e.g., Euros per hour) or qualitative (e.g., High, Medium, and Low). With this input data at hand for each resource (i) a business process-wide, local importance value, and (ii) an organization-wide, global importance value is calculated. While existing approaches

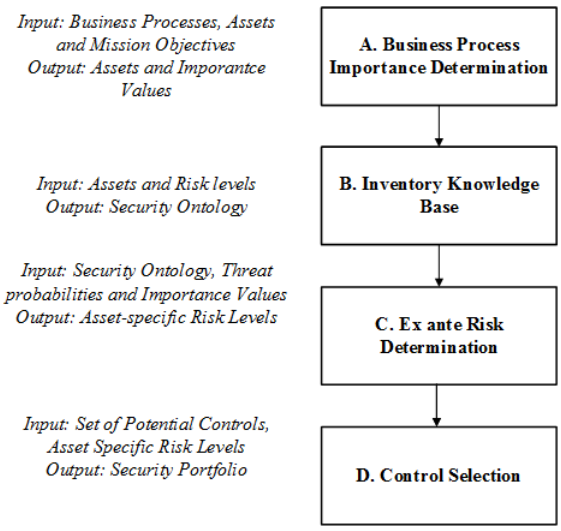

Figure 1. FORISK modules.

of importance determination (cf. [4]) do not incorporate dynamic aspects such as duration of activities and recovery times, we aim to integrate the time-factor as a crucial determinant of business process resilience [5].

B. Inventory Knowledge Base

In the early phase along the risk and resilience management cycle, an organization has to define (i) their assets, (ii) its corresponding acceptable risk levels, (iii) the organization-wide importance of the defined assets, and (iv) the attacker profile in terms of motivation and capability. To store and interrelate this information with general information security domain knowledge we use a security ontology. We utilize the security ontology by Fenz et al. [6], which is based on the security relationship model presented in the NIST 800-12. Transforming the advantages of formal specifications on the challenge of modeling security relationships results in the following three major advantages: (i) ontologies facilitate interoperability by providing a shared understanding of the domain in question and help to avoid heterogeneity, (ii) ontologies provide a formalization of shared understanding which allows for machine-processability, and (iii) ontologies support reusability as an important factor in information security risk management. Already gained information about the own company, including identified risks and applied actions, is of paramount importance for ongoing handling and maturity of the information security risk management process. Not only can the created data be reused in future projects, independently of implemented tools, but also can other groups, e.g., open communities facing similar risks in the same domain or partner organizations, profit from the collected data. The ontology follows the OWL-DL (W3C Web Ontology Language) standard and ensures that the knowledge is represented in a standardized and formal form to enable its utilization by automated systems. The introduced security ontology incorporates a basic set of concept definitions, relations, and formal axioms to generate an ontological model of the organization in the system characterization phase but has to be adopted to allow the use of ISO27001/27002 objects and filled with data.

C. Ex ante Risk Determination

In the phase, our approach extracts knowledge regarding threats, threat a priori probabilities, vulnerabilities, existing and potential control implementations, attacker profiles, and the assets of the organization from the security ontology and establishes a Bayesian network capable of calculating threat probabilities based on the aforementioned input information. In general 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. At this step it is important to compile a comprehensive list of potential threats (e.g., as recommended in [7]). While standards and best practices often provide an exemplary threat list, the risk manager is not always aware about the nature of each threat (which threats threaten critical assets? Which threat is a multiplier?) Such questions are hardly addressed in current information security risk management standards or best-practice guidelines. Starting from the threat report produced in the previous step, the vulnerability identification step analyzes potential vulnerabilities which are present in the defined system. This includes the consideration of vulnerabilities in the field of (1) management security (e.g., no assignment of responsibilities or no risk assessment), (2) operational security (e.g., no external data distribution and labeling or no humidity control), and (3) technical security (e.g., no cryptography solutions in use or no intrusion detection in place). For each threat highly granular vulnerabilities, which a threat could exploit, are defined and modeled in the ontology. For each of the vulnerabilities a mitigation control is assigned, thus implementing a control aim to close a vulnerability. With these functions in place, a user knows exactly how to protect his organization from specific threats: mitigating vulnerabilities by implementing recommended controls.

D. Control Selection

In this process step, controls which could mitigate or eliminate the identified risks, as appropriate to an organization's operations, are provided. In the control evaluation phase existing and potential control implementations, their effectiveness, initial and running costs are extracted from the security ontology. Information regarding the relevance of existing and potential control implementations is extracted from the Bayesian threat probability model. Using the extracted data as input for the interactive decision support methodology, we provide a methodology for two fundamental IS risk management questions (and a significant

extension to our previous work, cf. [8]: (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 cost-efficiently to an acceptable level? In contrast to traditional risk management processes, this solution provides a thorough knowledge base about countermeasures and thus (i) saves time, (ii) avoids that solutions are simply forgotten, and (iii) provides effective controls in compliance with best-practice standards. Furthermore, it supports decision makers to derive concrete security solutions based on the abstract control definition of the ISO 27001/27002 standard. However, with the list of potential control instances at hand, the decision makers still have to identify the optimal set of security solutions under economic considerations. Such cost-benefit analysis are still rarely considered by existing security standards such as NIST SP 800-30 and focus mainly on financial measures only.

IV. Attempted Evaluation and Future Work

As mindfulness, an organization's capability to perceive cues, interpret them, and respond appropriately [1], is crucial to maintain and enhance resilient operation, the project attempts to elaborate the conception and implementation of intuitive user interfaces based on exploratory mining techniques in order to evaluate the effectiveness of FORISK in real business cases. The contributions of these extending efforts will be twofold:

Firstly, the design of an automated "Business Process Resilience Detector" (BPRD) as an ex post-checking module will close the management-cycle of the FORISK architecture. In contrast to module C. Ex ante Risk Determination that attempts to calculate operational risks based on (either subjective or historical) threat probabilities (focus on the cause of events), the ex post detecting resilience will focus on the business processes' interdependencies and potential to cascade (focus on the impact). Thus, the complementary BPRD addresses further questions such as (1) Do the actual process models correspond with the intended concepts? (2) Does the observed system behavior meet requirements of the respective compliance standard? (3) Can we derive further information about the dynamic system behavior (e.g. recovery time, rate of degeneration)? In order to extract the interdependencies and dynamics, we will employ process mining techniques for conformance checking [9] as well as process discovery [10], [11].

Secondly, the user interface will allow us an evaluation of FORISK in collaboration with practitioners. After designing user interfaces in accordance with the requirements of the users (considering different user groups, such as chief process owner, who demands other information as the chief security officer), the focus will lie on the evaluation of the interfaces using state of the art devices that support an intuitive handling. The evaluation will rely on inspection (expert evaluation) and usability testing. Inspection will use Heuristic evaluation according to standards, guidelines and checklists and Cognitive Walkthroughs using typical task scenarios. Usability testing will use the Teaching Back method, benchmark tests comparing the interfaces with other approaches and Task-Performance analysis. The detailed usability evaluation in an early stage of the project should identify if decision makers accept the proposed methodologies and how the methodologies could be adopted in order to improve their acceptance in practice. Therefore, we will evaluate the prototypical implemented framework at two different companies. To ensure that the project results meet the needs of a broad range of companies we will evaluate the research results at one small- and one large-sized company in Europe.

References

[1] B. S. Butler and P. H. Gray, "Reliability, mindfulness, and information systems," *MIS Quarterly*, vol. 30, no. 2, pp. 211–224, 2006.

[2] P. D. for Business Enterprise and R. Reform, "2008 information security breaches survey." Tech. Rep., April 2008.

[3] R. A. Caralli, J. H. Allen, P. D. Curtis, and L. R. Young, *CERT resilience management model, version 1.0*. CMU, Software Engineering Institute, 2010.

[4] S. Fenz, A. Ekelhart, and T. Neubauer, "Business process-based resource importance determination," in *Conference on Business Process Management*, ser. LNCS, vol. 5701. Springer, 2009, pp. 113–127.

[5] C. W. Zobel and L. Khansa, "Quantifying cyberinfrastructure resilience against multi-event attacks," *Decision Sciences*, vol. 43, no. 4, pp. 687–710, 2012.

[6] S. Fenz and A. Ekelhart, "Formalizing information security knowledge," in *ACM Asian Symposium on Information, Computer and Communications Security*, 2009. ACM, 2009, pp. 183–194.

[7] S. Fenz, A. Ekelhart, and T. Neubauer, "Information security risk management: In which security solutions is it worth investing?" *Comm. AIS*, vol. 28, Art. 22, 2011.

[8] T. Neubauer, A. Ekelhart, and S. Fenz, "Interactive Selection of ISO 27001 Controls under Multiple Objectives," in *Information Security Conference*, ser. IFIP, vol. 278, 2008, pp. 477–492.

[9] R. Accorsi and T. Stocker, "On the exploitation of process mining for security audits: The conformance checking case," in *ACM SAC*. ACM, 2012, pp. 1709–1716.

[10] R. Accorsi, T. Stocker, and G. Müller "On the exploitation of process mining for security audits: The process discovery case," in *ACM SAC*. ACM, 2013, pp. 1462–1468.

[11] R. Accorsi, M. Ullrich, and W. M. P. van der Aalst, "Process mining," *Informatik Spektrum*, vol. 35, no. 5, pp. 354–359, 2012.