RiskFlows – Continuous Risk-driven Workflows and Decision Support in Information Security Management Systems

Michael Brunner

University of Innsbruck, Institute of Computer Science
Research Group Quality Engineering
6020 Innsbruck, Austria
michael.brunner@uibk.ac.at

Supervisor: Ruth Breu

Abstract. Information Security Management Systems (ISMS) aim at ensuring proper protection of information values and information processing systems (i.e. assets). Information Security Risk Management (ISRM) techniques are incorporated to deal with threats and vulnerabilities that impose risks to information security properties of these assets. Considering the evolution of information systems as well as more demanding security requirements, enterprises have to efficiently deal with changes to their assets, their risk exposure and the impact of these changes to their ISMS and ISRM activities. Current approaches are not well-suited for enterprises facing information security challenges from continuously evolving systems, diverse requirements regarding information security properties and regular changes to their assets and threat landscape. In our PhD thesis we will develop a continuous risk-driven approach to model and enact workflows in ISMS where security risks and derived controls are managed in a collaborative fashion. In this paper we present the problem statement, research goals, the applied methodology and expected contribution of our PhD thesis.

Keywords: Information Security Management Systems, Information Security Risk Management, Risk Modeling, Process Automation, Decision Support

1 Introduction

Information Security Management Systems (ISMS) aim at ensuring proper protection of information values and information systems regarding their confidentiality, integrity and availability. These information values and information processing systems are commonly referred to as assets and managing an asset model (or at least an inventory of all relevant assets) is a fundamental requirement for ISMS. Information Security Risk Management (ISRM) techniques are used to systematically identify security risks of these assets, analyzing and evaluating them and finding proper means to treat risks to information security. Most standards and best practices in the area of ISMS, ISRM and also Governance, Risk and Compliance Management (GRC) recognize the need to react to changes of the assets involved and the overall risk landscape an enterprise faces [1, 2]. The current practice, that is mandated by industry standards in this field, is to follow an audit-driven course of action and to reassess information security risks annually or when significant changes are planned (e.g., the ISO 27k family of standards [3, 4]). This naturally gives rise to challenges from efficiently dealing with changes to relevant asset models and related risks, especially in larger enterprises where multiple stakeholders are involved or even external parties have to be taken into account [5, 6].

Enterprises have been catching up on information security during the past five years and most of them have established a risk-based cybersecurity framework [7]. A major weakness is still their inability to reliably evaluate their actual risk exposure and to manage security controls from both a business and technology perspective. Another weakness is the mendable handling of the evolution of systems within information security management and risk assessment. These gaps in research and industrial practice have been recently asserted by the NIS Platform [8]. Furthermore, the current trends towards more flexible service supply chains, increasing usage of distributed services and an overall increasing complexity regarding information system composition call for a more dynamic and continuous approach to deal with risk in ISMS [9, 10].

A continuous approach has the potential to dynamically address such changes, providing decision support for involved stakeholders, offering automated ways to enact collaborative ISMS and ISRM workflows, or automating (parts of) common risk management tasks. Automation capabilities could range from workflow enactment as reaction to changes to completely automating risk assessment tasks. Ultimately, this includes enforcing appropriate security controls without direct stakeholder participation. Where stakeholder involvement is needed suitable techniques are to be employed that ensure that work load for individuals is minimized and collaboration between stakeholders is structured efficiently. We plan to develop a continuous ISMS approach that addresses the tight coupling of the three dimensions (1) change handling, (2) workflow automation, and (3) stakeholder collaboration.

This PhD thesis will follow a design-science research approach [11] to develop a framework for continuous risk-driven workflows and decision support in ISMS to address current challenges with regard to changes of the system under investigation, the operational environment and the actual threat landscape. The final goal is to provide a general framework that establishes support for highly automated workflows to identify risks, analyze them and choose appropriate risk treatments in accordance with configurable information security policies.

2 State of the Art

Many standards and best practices in the area of information security management (e.g., ISO 27001 [4], Common Criteria for Information Security Evaluation [12], IT Baseline Protection Catalogues [13], ITIL [14], COBIT [15]) require the definition and establishment of risk management processes. Typically ISMS standards do not offer clear direction towards the risk assessment methodology that should be applied and merely state requirements regarding documentation artifacts and the design of the risk management process.

The coupling between security requirements, security controls and risk management generated different solutions to model risk and derive security controls as means of risk mitigation. Risk assessment captures methods and techniques aiming at identification of risks, analyzing their causes and consequences and estimating their probability and impact [3]. On one side, approaches such as the Failure Mode and Effect Analysis (FMEA), Hazard and Operability Study (HAZOP) or Preliminary Hazard Analysis (PHA) tend to rely heavily on stakeholder knowledge. The used models of investigated assets, vulnerabilities and threats are more simplistic, do not always model interrelations precisely, and therefore require less effort upfront. On the opposite side more formal techniques for risk assessment stem from tree-based approaches (e.g., fault tree analysis, attack trees) or utilize probabilistic methods (e.g., Markov Chains, Monte Carlo Simulation) and thus require more detailed models. Techniques such as the Cyber Security Modeling Language (CySeMoL) [16, 17] or ISMS-CORAS [18] put special attention to model risks in the scope of whole enterprises based on specific enterprise architecture models. The downside of these approaches is that detailed enterprise models are a prerequisite and that the use of predefined model elements is enforced, which might not be compatible with already existing enterprise architecture modeling initiatives.

Approaches dealing with changes of systems and threat scenarios primarily target traceability aspects, e.g., within and between risk models and asset models and additionally address the detection of model changes. Consequently, inconsistencies introduced by changes and modularization of security analysis as counteraction have been investigated for certain areas such as access control or the domain of safety engineering [10, 19]. The utility of this approaches for ISRM in a collaborative environment with multiple stakeholders being involved have not yet been demonstrated.

Looking into business processes and workflow management Suriadi et al. [20] give an overview of existing risk-based approaches. Basically, frameworks such as presented in [21–23] employ a notion of risk to monitor and analyze workflows and workflow instances, but do not use risk as a workflow controlling entity. Instead they combine a risk management cycle with process modeling tasks with the ultimate goal to incorporate risk monitoring into process execution.

Collaborative security management has been thoroughly researched in the past years [24, 25]. Although these approaches address issues from and within collaborative processes to manage information security and also partly cover aspects from risk assessment, they do not establish means for automation or risk-based workflows.

3 Research Objective and Questions

The research objective of this PhD thesis is to *develop a solution for continuous risk-driven ISMS* that is (1) capable of *systematically handling changes* within asset and risk models, (2) *provides suitable automation facilities* to reduce costs and (3) *efficiently organizes stakeholder collaboration.* We envision a general framework that establishes support for highly automated workflows to identify risks, analyze them and choose appropriate risk treatments (thus risk-driven). The primary goal is to enable enterprises to react to relevant changes of the threat landscape or their operational environment faster than existing approaches allow them to. Our solution will consist of a framework and the implementation of an accompanying software tool.

To achieve our overarching goal we will provide answers to the following research questions:

- **RQ1: Which automation techniques are used in ISRM within enterprises operating an ISMS?** We want to shed light into the risk management techniques employed by enterprises that operate an ISMS and better understand why and how certain tasks are automated and others are not. This will help us to better understand the prerequisites (e.g., processes, models, data sources) for successful automation in ISRM.
- **RQ2: What are workflows to systematically deal with change for continuous risk-driven ISMS?** Since we aim at developing a continuous approach it is of utter importance to efficiently deal with changes to the asset and risk model. Considering that a fully automated approach is not always possible or desired, we will develop a selection of workflows to deal with change including effective organization of stakeholder collaboration.
- **RQ3: Which individual ISRM tasks benefit the most from enhanced automation within a continuous risk-driven ISMS?** Our goal is to develop a continuous risk-driven ISMS and we aim at increasing the automation of risk management tasks. Currently we see the most promising tasks being automated risk estimation (defining probability and impact for individual risks) and risk treatment (e.g., instantiation of security controls). However, we also want to research automation possibilities for other ISRM tasks and how well they fare within a continuous ISMS.

4 Research Design and Methodology

To answer our research questions and to reach our overarching goal we will conceptualize a framework and build an accompanying software tool to enable automated workflows and decision support based on continuous risk management for ISMS – *RiskFlows*. We will follow the principles of design science research [11]. Where aspects of Human Computer Interaction (HCI) are involved, we will incorporate notions of concept-driven interaction design research methodology [26].

4.1 Planned Tasks

As first part of our work we will conduct two surveys: (1) a structured literature review concerning the current state of automated approaches in risk management which are used by or at least suitable for ISMS and (2) a survey of current industrial practice regarding automation in risk management of information security management. The survey regarding current industrial practice is planned as online questionnaire. Performing these surveys ensures adherence to the principals of problem relevance and research rigor demanded by design science research. These surveys will help us answering RQ1 and the results will also provide a suitable classification schema and a referential framework to assess identified approaches. Furthermore, we will conduct expert interviews to derive key use cases for automation support together with their related activities, involved stakeholders and develop functional requirements for these use cases.

The results of the conducted surveys will be incorporated into our RiskFlows framework. The framework will constitute of partaking stakeholders/roles, process models, required documentation artifacts and an applicable risk analysis methodology to best support automation and decision support for the envisioned application context. The framework itself will be tool-agnostic and the prime design artifact of our work (following the design science principle of providing an artifact) and provide answers for RQ2 and RQ3. Furthermore, we will define a prioritized set of use cases for our framework, evaluation criteria regarding support for each individual use case and maturity of their realization in preparation for the next tasks. As evaluation criteria we will develop a set of Key Performance Indicators (KPI) [27]. We plan on extending and verifying the evaluation criteria by means of expert interviews with professionals from academia and industry.

In order to demonstrate the utility, quality and efficiency of our RiskFlows framework we will implement an accompanying tool and then examine the applicability of our approach via a near-life usage scenario. This usage scenario will be developed in close cooperation with industry partners. The final stage of our work will be a evaluation of RiskFlows. We will perform the evaluation based on previously identified use cases and the developed KPIs. The prototype together with the near-life usage scenario will be provided to experts from academia and industry for this evaluation. The evaluation results will be used to reflect upon the devised framework and point out possible future enhancements.

4.2 Proposed Solution RiskFlows

As prerequisite for RiskFlows we require enterprises to provide an asset model of the system under investigation that is tightly coupled with the actual realization of these systems. These asset models will be automatically imported and updated from (potentially multiple) available data sources such as enterprise architecture models and configuration management databases. Starting from this asset model, our approach will automatically steer and enact ISMS-related workflows and ensure proper and timely cooperation between stakeholders. Our focal point will be put on processes for risk assessment, including the areas of risk identification, analysis and evaluation.

RiskFlows will consume/interface the aforementioned asset model of the system under investigation and a threat model providing the threat landscape to be examined. Changes to the system under investigation (e.g., integration of new IT service, addition of infrastructure components, roll-out of new software version) as well as changes to the threat landscape (e.g., new exploits identified, additional incidents detected) will be continuously monitored. When relevant changes emerge, RiskFlows will enact predefined workflows that trigger corresponding risk-assessment activities (e.g., update risk probability/impact, enforce risk mitigation strategy) that are either performed fully automatic or relapse to a semi-automatic solution where stakeholder participation is stipulated. RiskFlows will ensure proper integration of stakeholders where needed and provide them with the required dataset to make informed decisions regarding risk evaluation and risk treatment.

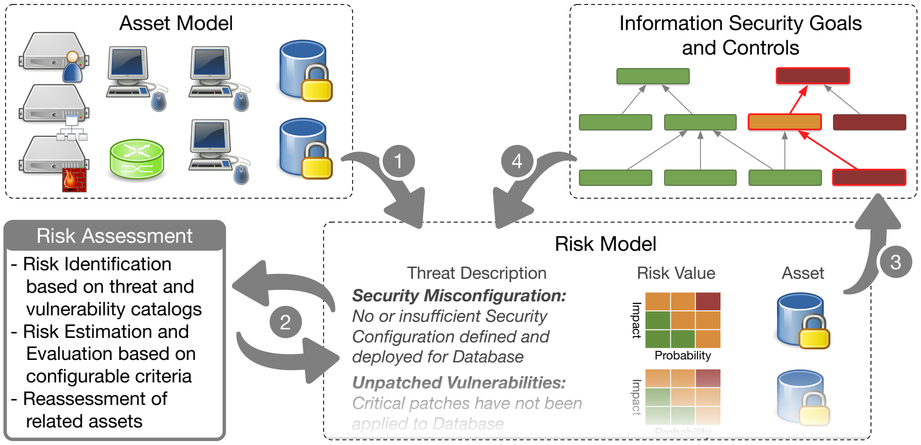
Asset Model
Information Security Goals and Controls
1
4
Risk Assessment
- Risk Identification based on threat and vulnerability catalogs
- Risk Estimation and Evaluation based on configurable criteria
- Reassessment of related assets
2
3
Risk Model
Threat Description
Risk Value
Asset
Security Misconfiguration:
No or insufficient Security Configuration defined and deployed for Database
Impact
Probability
Unpatched Vulnerabilities:
Critical patches have not been applied to Database
Impact
Probability

Fig. 1. RiskFlows Example

Figure 1 illustrates a simplified RiskFlows example: The starting point is the addition of a new database to the asset model (1). RiskFlows detects this change and ensures that the risk model is updated accordingly by conducting an automatic risk assessment (2). The considered threats and vulnerabilities for the new asset are derived from predefined catalogs and instantiated. RiskFlows then estimates and evaluates these risks in accordance with the configured criteria for impact and probability of each risk. Due to assets being connected with each other this step might require the reassessment of risks from connected assets as well. Following the risk assessment RiskFlows will instantiate additional security controls to address newly identified risks (3). Finally RiskFlows will re-evaluate risks when controls have been successfully implemented (4).

To achieve this, we will provide a tailored risk assessment methodology that supports automated risk identification based on asset and threat models as well as automated estimation of risk impact and probability. Typically impact will be derived from the business side whereas probability for certain risks will highly depend on technical matters. Taking complex multi-layered asset models into account, our methodology will offer guidance on how to decompose risk impact from the business layer down to the infrastructure layer and offer means to condense probabilities from more technical layers upwards to the business layer in return. As example, the business impact from reduced availability of an IT service must be decomposed in a way that the fraction of the impact resulting from required infrastructure components (e.g., servers running parts of the IT service) can be estimated. On the other hand, the probability of failing infrastructure components must be condensed upward such that a veridic estimation of the dependent IT service not meeting the availability constraints can be made. In order to configure these aspects we will develop a formal information security policy language that will be used to define the behavior of RiskFlows.

We will place our approach within the normative references of the standards ISO 27001 [4], regarding information security management and ISO 27005 [3] for information security risk management to ensure compatibility with current industry standards. RiskFlows will be conceptualized and eventually realized as extension of ADAMANT [28] which at its current state provides basic ISMS functionality regarding the management of security requirements and controls as well as preliminary workflow support. RiskFlows will enhance ADAMANT by addition of the risk management features (including automated risk assessment) and risk-driven workflows.

4.3 Expected Contribution and Current State of the PhD Thesis

With our survey we will be able to gain a *better understanding of the prevailing ISRM approaches used by ISMS practitioners* and their suitability for automating workflows or providing decision support in ISMS. This should prove useful for a wider audience since the current scientific exploration of the industrial practice regarding RM techniques used in information security management is highly fragmented. With RiskFlows we will provide a *novel risk-driven approach to model and enact workflows in ISMS where information security risks and derived controls are continuously managed* as opposed to the audit-driven course of action utilized by most enterprises at the moment. We will provide the conceptual framework as well as a prototypical implementation to interested parties for further evaluation. Furthermore, we will use the evaluation of RiskFlows to show that a continuous approach underpinned by automated workflow enactment is better suited to tackle core ISMS and ISRM tasks.

At the time of writing we are preparing and conducting initial surveys and expert interviews providing the basis for our future work on the conceptualization of the RiskFlows framework. Furthermore, we are implementing required enhancements for ADAMANT such as support for modeling risks, associated workflows and import mechanisms for asset models form multiple data sources.

5 Conclusion

With our PhD thesis we intend to leverage the fundamentals for a continuous risk-driven approach to model and enact workflows in ISMS where security risks and derived controls are managed in a continuous fashion. Our ultimate goal is to enable enterprises to immediately and adequately react to relevant changes in threat landscape and the operational environment. Therefore, our approach emphasizes automation of ISMS workflows, especially the potentially automated risk evaluation and risk treatment for the system under investigation.

References

1. H. Abbas et al. “Addressing dynamic issues in information security management”. In: *Information Management & Computer Security* 19.11 (2013), pp. 5–24.
2. D. W. Straub and R. J. Welke. “Coping with systems risk: Security planning models for management decision making”. In: *MIS Quarterly* 22.44 (1998), pp. 441–469.
3. ISO. *ISO/IEC 27005: Information technology – Security Techniques – Information security risk management.* 2011.
4. ISO. *ISO/IEC 27001: Information technology – Security techniques – Information security management system – Requirements.* 2013.
5. S. Thalmann et al. “Challenges in Cross-Organizational Security Management”. In: *System Science (HICSS), 2012 45th Hawaii International Conference on* (2012), pp. 5480–5489.
6. R. P. Tracy. “IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards”. In: *Information Systems Security* 16.22 (2007), pp. 114–122.
7. PWC. *The Global State of Information Security®Survey 2016.* 2015.
8. NIS Platform. *State-of-the-Art of Secue ICT Landscape.* 2015.
9. D. Bachlechner, S. Thalmann, and R. Maier. “Security and compliance challenges in complex IT outsourcing arrangements: A multi-stakeholder perspective”. In: *Computers & Security* 40 (2014), pp. 38–59.
10. A. Borek et al. “Managing information risks in asset management - Experiences from an in-depth case study in the utility industry”. In: *Asset Management Conference 2011, IET and IAM* (2011), pp. 1–6.
11. A. R. Hevner et al. “Design science in Information Systems research”. In: *MIS Quarterly* 28.11 (2004), pp. 75–105.
12. The Common Criteria Recognition Agreement Members. *Common Criteria for Information Technology Security Evaluation.* 2006.
13. German Federal Office for Information Security. *IT Baseline Protection Catalogues.* 2008.

14. J. O. Long. *ITIL®2011 at a Glance.* 2012.
15. IT Governance Institute. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* 2012.
16. H. Holm et al. “CySeMoL: A tool for cyber security analysis of enterprises”. In: *Electricity Distribution (CIRED 2013), 22nd International Conference and Exhibition on* (2013), pp. 1–4.
17. T. Sommestad, M. Ekstedt, and H. Holm. “The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures”. In: *Systems Journal, IEEE* 7.33 (2013), pp. 363–373.
18. K. Beckers et al. “ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System.” In: *Engineering Secure Future Internet Services and Systems* 8431 (2014), pp. 315–344.
19. L. Montrieux, M. Wermelinger, and Y. Yu. “Challenges in model-based evolution and merging of access control policies”. In: *the 12th international workshop and the 7th annual ERCIM workshop* (2011), pp. 116–120.
20. S. Suriadi et al. “Current research in risk-aware business process management : overview, comparison, and gap analysis”. In: *School of Electrical Engineering & Computer Science; School of Information Systems; Science & Engineering Faculty* (2014).
21. S. Betz, S. Hickl, and A. Oberweis. “Risk-Aware Business Process Modeling and Simulation Using XML Nets”. In: *Commerce and Enterprise Computing (CEC), 2011 IEEE 13th Conference on* (2011), pp. 349–356.
22. R. Conforti et al. “A software framework for risk-aware business process management”. In: *Institute for Future Environments; School of Information Systems; Science & Engineering Faculty* (2013).
23. S. Tjoa, S. Jakoubi, and G. Quirchmayr. “Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modeling and Simulation Methodology”. In: *2008 Third International Conference on Availability, Reliability and Security* (2008), pp. 179–186.
24. M. Hawley et al. “Collaborative Security Management: Developing Ideas in Security Management for Air Traffic Control”. In: *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on* (2013), pp. 802–806.
25. F. Innerhofer-Oberperfler, M. Hafner, and R. Breu. “Living security collaborative security management in a changing world”. In: *Tenth IASTED International Conference on Software Engineering SE 2011* (2011).
26. E. Stolterman and M. Wiberg. “Concept-Driven Interaction Design Research.” In: *Human-Computer Interaction* 25.22 (2010), pp. 95–118.
27. D. Parmenter. *Key Performance Indicators(KPI), developing, implementing and using KPIs.* 2010.
28. M. Brunner and R. Breu. “IT Compliance mit kontextuellen Sicherheitsanforderungen”. In: *D.A.CH Security 2014* (2014), pp. 136–147.