

Mueller, I., Han, J., & Schneider, J.-G., et al. (2011). Idea: a reference platform for systematic information security management tool support.

Originally published in U. Erlingsson, R. Wieringa, & N. Zannone (eds.). *Proceedings of the 3rd International Symposium on Engineering Secure Software and Systems (ESSoS 2011), Madrid, Spain, 09–10 February 2011.* Lecture notes in computer science (Vol. 6542, pp. 256–263). Berlin: Springer.

Available from: http://dx.doi.org/10.1007/978-3-642-19125-1_20

Copyright © 2011 Springer-Verlag Berlin Heidelberg. The original publication is available at <u>www.springer.com</u>.

This is the author's version of the work. It is posted here with the permission of the publisher for your personal use. No further distribution is permitted. If your library has a subscription to these conference proceedings, you may also be able to access the published version via the library catalogue.



Idea: A Reference Platform for Systematic Information Security Management Tool Support

Ingo Müller¹, Jun Han¹, Jean-Guy Schneider¹, and Steven Versteeg²

¹ Swinburne University of Technology, Hawthorn, Victoria 3122, Australia {imueller,jhan,jschneider}@swin.edu.au

² CA Labs, CA Technologies (Pacific), Melbourne, Victoria 3004, Australia steve.versteeg@ca.com

Abstract. The ISO 27001 standard specifies an information security management system (ISMS) as a means to implement security best practices for IT systems. Organisations that implement an ISMS typically experience various challenges such as enforcing a common vocabulary, limiting human errors and integrating existing management tools and security mechanisms. However, ISO 27001 does not provide guidance on these issues because tool support is beyond its scope, leaving organisations to start "from scratch" with manual and usually paper document-driven approaches. We propose a novel reference platform for security management that provides the foundation for systematic and automated ISMS tool support. Our platform consists of a unified information model, an enterprise-level repository and an extensible application and integration platform that aid practitioners in tackling the aforementioned challenges. This paper motivates and outlines the key elements of our approach and presents a first proof-of-concept prototype implementation.

1 Introduction

The ISO 27001 standard [1] specifies a well-defined process for implementing and operating an enterprise-level information security management system (ISMS). This ISMS establishes security best practices for an IT system based on (i) systematic risk assessment, (ii) coordinated design and implementation of controls and (iii) ongoing assessment of the effectiveness of these controls. The benefits of an ISMS are increased transparency of security management decisions and their alignment with their system-level implementation. Hence organisations gain better understanding of the security posture of their IT systems enabling them to better protect their information assets and to demonstrate due diligence.

However, as we have learnt from practitioners, reaping these benefits is challenging because of a lack of tool support. ISO 27001 and the related ISO 27003 standard [2] specify a manual document-driven process with tool support out of their scope. Moreover, existing tools such as for governance, risk and compliance (GRC) or risk management focus on specific aspects, to the best of our knowledge, but do not cover the entirety of the implementation and operation of an ISMS. Due to this lack of support, organisations typically start "from scratch" with manually managed paper documents and experience challenges, such as:

- 1. Difficulties to establish and enforce a common vocabulary across the departments and different hierarchy levels of an organisation;
- 2. Difficulties to limit human impact (errors, inconsistencies and omissions) on security management activities;
- 3. Lack of standard-compliant support for the integration of "local" security management tools and enforcement mechanisms with the "global" ISMS.

Consequently, an ISMS may not enforce security best practices effectively and additional time, resources and investments may be required to establish ISO 27001 compliance. The goal of our work is to address the above challenges and to support organisations to obtain ISO 27001 certification. We propose a novel security management platform that provides the foundation for systematic and automated ISMS tool support. The platform comprises three key elements: a unified information model, an enterprise-level information repository and an extensible application and integration platform. These elements address the three challenges above. Our platform is defined as a generic and system-independent reference platform that can be applied by any organisation to augment their ISMS with automated tool support, respectively.

In this paper, we motivate and outline the elements of our reference platform in Section 2 and present a proof-of-concept-prototype in Section 3. The paper concludes with a summary and an outlook to future work in Section 4.

2 Security Management Reference Platform

Our approach is fully aligned with ISO 27001. Thus, this section motivates and presents the key elements of our approach driven by ISO 27001 features and highlights how these elements help to alleviate the aforementioned challenges.

2.1 Unified Information Model

ISO 27001 requires the creation of a common vocabulary that supports the unambiguous definition of security policies and procedures across all units of an organisation. The objective is to unify and align the views of all involved stakeholders. For example, the CIO views access control from the management perspective, considering the number of incidents and their impact on the business, whereas a system administrator is concerned with technical aspects such as password strength and monitoring audit trail records.

The challenge of a manual paper-based approach is twofold. Firstly, it is difficult to establish and synchronise a common vocabulary across documents due to varying authorship and document-specific glossaries. Secondly, it is difficult to enforce that stakeholders adhere to the vocabulary when creating or modifying documents due to lacking means to verify inputs immediately as they are written.

We propose a unified information model to tackle this challenge. An information model specifies concepts, their relationships and operations to define the semantics of a problem domain. We have developed an information model for



Fig. 1. UML class diagram of the information model main concepts.

the information security management (ISM) domain based on ISO 27001 that supports information exchange and management activities across different stakeholders, departments and management applications. Our information model is depicted in Figure 1. It is structured into sub-models, each containing concepts that pertain to a concrete ISM activity. Every concept comprises informally (in natural language) and formally (in formal languages) specified attributes. In this way, management-level requirements and decisions are aligned with system-level configurations, system properties and enforcement mechanisms. The information model is specified using object-oriented concepts and UML formalisms to enable machine processing of concrete representations and their customisation by taking advantage of inheritance and polymorphism features. The details of the information model are specified in [3].

Our information model mitigates the challenge of managing a common vocabulary. Firstly, it enables organisations to systematically specify a unified vocabulary for all aspects related to their ISMS in a fine-grained and electronic fashion based on *ISM concepts* rather than documents. Secondly, tools can be developed that enforce the correct use of the vocabulary during the creation or modification of concepts based on the information model. For example, Figure 2 depicts the input mask of a graphical user interface (GUI) for the manipulation of information about metrics (*e.g.* a metric for measuring the effectiveness of an access control mechanism). The GUI indicates mandatory information and enforces vocabulary-compliant inputs with dedicated input elements (*e.g.* multiple-choice combo boxes) and input filters (*e.g.* to verify the temporal correctness of *Start Date* and *End Date*). Figure 2 also demonstrates how the information model aligns management-level and system-level views of a concept (*cf. Outline* text field with the prefix algebraic expression of the *Function* text field).

2.2 Enterprise-level Repository

ISO 27001 specifies a document-driven process to ISM. These documents are created by various stakeholders throughout the organisation and modified over time with the objective to reflect the actual state of an ISMS implementation at any time. For example, an organisation documents all access control points including their potentially department-specific configurations and constraints.

The challenge of a manual paper-based approach is twofold. Firstly, it is difficult to keep all documents up to date such that they reflect the actual state of the ISMS. Secondly, it is difficult to ensure that the documents, individually and across different documents, remain coherent, correct and as complete as possible. In other words, it is difficult to limit the human impact on security management activities, such as errors, inconsistencies and omissions.

We propose an enterprise-level information repository to address this challenge. The repository captures, consolidates and correlates security-related information across different stakeholders, departments and management applications. It is structured based on our information model and, thus, ensures correctness and durability of the instances of information model concepts as well as the referential integrity of their associations. The repository also implements capabilities for managing security-related information including unique identification, access control, version control and meta-information management.

The repository enables keeping organisation-wide security-related information coherent, correct and complete. Firstly, all information is consolidated and correlated centrally. In this way, redundancies are avoided and ISO 27001-relevant documents can be generated from the same data. Secondly, the data dictionary of the repository can be used to develop tools to raise alerts in case inputs

	Create Metric	
Outline	The number of deactivated user accounts	Version Information
Description	The aim of this metric is to assess if all	Creator psmith
Security Functions	restrict access with secure log-on procedure for all user accounts Select	Approver - Version 1 Timestamp 2010-04-16 16:29:51.494
Start Date (dd/mm/yyyy)	1 • 1 • 2010 • (hh:mm:ss) 23 • 59 • 0 •	Status submitted
End Date (dd/mm/yyyy)	31 v 12 v 2010 v (hh:mm:ss) 0 v 0 v	
Collecion Period	start-date=23.59:1/1/2010, quantity=1, fixed-period-point=day	Classification Information
	Add Remove	ISO/IEC 27002:2005(E),11.6.1 NIST 800-53 revision 3,AC-3
Metric Scope	Execution	
Metric Target	Product	
Metric Type	Atomic	Select
Function	DIV(E1.A1,E2.A2)	
Value Type	Rate	Access Control Information
Value Scale	· · · · · · · · · · · · · · · · · · ·	

Fig. 2. Screenshot of the input mask for metric definitions.

are incorrect, inconsistent or incomplete at the time of input. For example, see Figure 2 for a GUI that enforces the input of all mandatory attributes of the metric concept, thus preventing omissions. It contains input filters (*e.g.* to verify the correctness of the *Collection Period*) and dedicated input elements (*e.g.* multiple-choice combo boxes) to avoid errors and reduce inconsistencies. This GUI can be auto-generated based on the repository's data dictionary.

Additional input checkers are feasible that inspect user inputs to verify syntactic and semantic correctness, *e.g.* for the *Function* text field in Figure 2. Moreover, tools for change management and impact analysis can support the identification of concepts in the repository that are affected by a change by tracing concepts via their associations. Finally, instead of a human reading through a set of documents, the repository supports automated queries for identifying rogue data sets that contain incorrect, incomplete or outdated information.

2.3 Extensible Application and Integration Platform

ISO 27001 does not provide explicit guidance for infrastructure and tool support for an ISMS. Hence, organisations need to develop required IT system support from scratch, for example for integrating log files and audit trails of access control points for the sake of measuring their effectiveness on an ongoing basis.

The challenge of a manual document-driven approach is that it is difficult to utilise existing security management tools and security enforcement mechanisms



Fig. 3. a) conceptual platform architecture and b) metric management workflow.

in a systematic and automated fashion such that security best practices are implemented as effectively as possible.

We propose an extensible application and integration platform that tackles this challenge following a generic Service-oriented management framework as outlined in Müller et al. [4]. The conceptual architecture of the platform is presented in Figure 3 a. It exhibits the characteristics of a *hub-spoke architecture*. The centrepiece, or hub, is an Enterprise Service Bus (ESB) that enables uniform message-oriented integration. Hence, the ESB provides the ideal foundation for integrating security management tools, applications, mechanisms and enforcement points. It facilitates interoperability and seamless exchange of data, events between them and supports overarching management activities.

The spokes of the architecture are a set of extension components as outlined below and two default components: Scheduler and Workflow Engine. The *Scheduler* component facilitates the automated scheduling of management workflows on the ESB. The *Workflow Engine* enacts and executes *management workflows*. A management workflow composes the functionality of sets of ESB components. Figure 3 b presents the representation of a generic management workflow for the automated collection, calculation, analysis and storage of metric data.

The platform can be extended with components that implement the following roles. The *Client role* describes the ability to integrate interfaces to humans and systems, *e.g.* a dashboard for administering the integration platform or inspecting the contents of the repository. The *Adapter role* describes the ability to integrate remote data sources and data sinks, management tools and applications. The enterprise-level information repository is integrated with the ESB using a component implementing this role. The *Capability role* describes the ability to integrate generic management functionality locally in the form of plug-ins. Components of this role typically manipulate information in the repository and interact with Adapter and Manager components. The Scheduler and Workflow Engine components embody the Capability role. The *Manager role* describes the ability to integrate remote management functionality that is situated in the managed IT system, as for example policy enforcement points or system moni-



Fig. 4. Auto-generated status report with scorecard.

tors. Furthermore, the platform offers an API for programming, integrating and managing components and deploying management workflows on the ESB.

The platform enables systematic and automated tool support. It facilitates the integration and interoperation of security management tools and enforcement mechanisms. It fosters information sharing and consistent data management across ISM activities. For example, Figure 4 illustrates a status report that was created based on (i) repository data, (ii) the execution of the management workflow in Figure 3 b and (iii) another generic workflow that automatically generates scorecards and a status report about the effectiveness of a specific access control point, and disseminates this report via e-mail to all involved stakeholders.

3 Proof-of-concept Prototype

We have devised a basic application scenario in order to implemented a prototype of the proposed security management platform. Consider the case where a new law requires hospitals to provide patients with online access to their medical records. Due to the high sensitivity of medical records, various regulations mandate access restrictions to protect the privacy of patients. Thus hospitals must ensure that this online access is secured also and managed with their ISMS.

Figure 5 depicts the design of a Web application that allows patients to interact with the *Patient Record Service* (PRS) in order to access their medical records stored in the *Patient Record Database* (PRDB). Figure 5 also shows the design of a concrete implementation of our reference platform including all components required to implement the conceptual architecture and workflow shown in Figure 3. Moreover, the current prototype implementation contains components that implement another workflow, as outlined in the previous section, that creates status reports and disseminates them to involved stakeholders. The functionality of our approach is illustrated with a basic use case scenario. Figure 2 presents an input screen that allows security experts and other stakeholders to define a metric and setup the automated collection and reporting of metric data. In this use case scenario, a metric is defined for measuring the effectiveness of the ACM component that protects online access to the PRS (*cf.* Figure 5). Figure 4 depicts a screenshot of a corresponding auto-generated status report.



Fig. 5. Modified UML deployment diagram of the prototype implementation.

4 Summary and Outlook

This paper proposed a reference platform that forms the foundation for systematic and automated tool support for the implementation and operation of an ISMS in alignment with the ISO 27001 standard. Our goal is to aid practitioners to overcome challenges of present typically manual and paper document-driven approaches. A proof-of-concept prototype has been developed to demonstrate our approach. Our next steps include the implementation of a realistic industry scenario to gain further insights, refine and validate our approach in collaboration with practitioners. Moreover, we will explore further tool support, *e.g.* how model-driven engineering methods can be utilised to automate the development, configuration and deployment of security mechanisms based on our approach.

Acknowledgements This work is supported by the Australian Research Council and CA Technologies (CA Labs). We also gratefully acknowledge Abhijat Sinha and Swapnil Raverkar who contributed to the implementation of the prototype.

References

- 1. ISO/IEC: Information technology Security techniques Information security management systems Requirements. 1st edn. (2005) ISO/IEC 27001:2005(E), International Standard.
- ISO/IEC: Information technology Security techniques Information security management system implementation guidance. 1st edn. (2010) ISO/IEC 27003:2010(E), International Standard.
- 3. Müller, I.: The Information Security Management Information Model (ISM-IM). Technical Report. Swinburne University of Technology (2010) http://www.swinburne.edu.au/ict/research/cs3/rsr/pubs/ISM-IM.pdf.
- Müller, I., Han, J., Schneider, J.G., Versteeg, S.: A Conceptual Framework for Unified and Comprehensive SOA Management. In Feuerlicht, G., Lamersdorf, W., eds.: ICSOC 2008 International Workshops, Revised Selected Papers. LNCS 5472, Sydney, Australia, Springer (2009) 28–40