Risk Management in the context of Information Security: a Model-Driven approach

ANACLETO CORREIA[1], ANTÓNIO GONÇALVES[2], and M. FILOMENA TEODORO[1],[3]
[1]CINAV, Portuguese Naval Academy, Alfeite, 1910-001 Almada, PORTUGAL.
[3]INESC-ID, Instituto Superior Técnico, Avenida Rovisco Pais, 1, 1048-001 Lisboa, PORTUGAL
[3]CEMAT, Instituto Superior Técnico, Avenida Rovisco Pais, 1, 1048-001 Lisboa, PORTUGAL
cortez.correia@marinha.pt

Abstract: - Information security is concerned with the requirements of availability, integrity, and confidentiality of information's assets, which are fundamental to the long-term survival of an organization. Information security relies in risk management for security risks identification, evaluation and treatment, according to the ISO 31000. The methodologies supporting information security implementation, such the ones based on the ISO 27000 set of standards, are holistic approaches that deals with corporate systems, as well as an extended network that includes business partners, vendors, customers and other stakeholders. This paper uses the model-driven approach for addressing information security systems conception and design, deemed to be compliant with the ISO/IEC 27000 and the ISO 31000 set of standards. A domain level model (computation independent model) based on the information security and risk management vocabulary present in the standards was built. This CIM model serves as a meta-model for platform independent models of information security systems compliant with the information security and risk management standards. This model is the baseline for conceiving, implementing and testing actual information security systems, allowing users from different organizational, functional, and technical levels to use a common language when embedding information security and risk management in their processes.

Key-Words: - information security, risk management, model-driven architecture, MDA.

1 Introduction

Organizations and their systems own sensitive information, which is critical to attain their objectives. Not infrequently, news came up notifying major theft or loss of key business data, with the regular organizations' operations compromised or even interrupted. In some cases, these events lead to the organization's major market value loss or, in the worst cases, to the organization's bankruptcy due to an irreversible damage on operations or reputation. Likewise, general public regularly experiences breaches in their privacy with phenomena such as online fraud or theft of personal identity.

Internal and external factors can turn uncertain whether a system or organization will achieve its objectives. The uncertainty that conditioning the accomplishment of an entity's objectives is *risk*. Another way of see risk is as the possibility of occurrence of an event that can reduce the value of the business. To deal with the potential losings underlying risk, one must manage it.

According to the ISO 31000:2009, to be manage, risks must be identified, analyzed and evaluated regarding requirements of modification, and subject to adequate treatment, in order to satisfy an predefined criteria. Therefore, the risk management process, undergoes through communication and consultation of stakeholders, as well as monitoring and review of risks and controls that mitigate the drawbacks in order to ensure that risks are maintained at an acceptable level [1].

The process of risk management can be tailored to different approaches in several domains (e.g. information security, finance, health). One can use risk management at a broad level (the whole organization), or at more restrict levels (at departmental or functional areas, projects and activities).

Information Security (IS), on the other hand, deals with the confidentiality, integrity, and availability of the information. In the information security perspective, the focus is the whole organization, including the assets that constitute the organization's corporate systems, supporting both the internal collaborators, as well as the business partners, vendors, customers and other stakeholders.

It is difficult for an organization to operate in today's technological context without an effective information security. Poorly-secured organizations, end up becoming threats to their partners. In the same way, consumers' confidence in an organization, would also depend, on the safety belief of their personal data. Furthermore, legislation and regulation make firms criminally liable, and in some instances directors personally accountable, for failing to implement and maintain appropriate risk control and information security measures.

Since the extent and value of information are continuously growing, the exposure of organizations and individuals to data misuse or destruction will tend to grow. The dissemination of increasingly complex, sophisticated and global threats to information security, in combination with the compliance requirements of the computer and privacy-related regulation, is driving to a more holistic view of organizations regarding information security [2].

For decision-makers, at all levels of the organization, it is fundamental to understand how to deal with information security risks. Only a comprehensive and systematic approach can deliver the level of information security that an organization needs. This approach is given by the international reference for information security management, i.e. the series of ISO/IEC 27000 standards on information security.

The ISO/IEC 27001 [3] is the key standard in the series. Compliance with this standard should enable an organization to demonstrate a proper response – to customers, suppliers, as well as to the regulatory and judicial authorities – to the challenges regarding information security risks.

In this paper, we take the Model Driven Architecture (MDA) [3] approach to risk management and information security in order to address the complexity of conceiving and implementing an information security system.

The MDA is an approach that aims to express the relevant concepts of a particular domain, through models. A model of a system, which is often presented as a combination of drawings and/or text, is a specification of the system and its environment for some certain purpose [3]. In this work, by using a model to describe information security systems, we provide a high-level non-technical view of the system, shared by all participants involved in risk management and information security system enactment and usage.

This work is presented in three sections. In the next section, we discuss the general approach of MDA. Following we delve into the specification of risk management and information security systems suitable for be instantiate in any organization. In the last section, we analyze the results and draw some conclusions.

2 The Model-Driven Approach

The Model-Driven Architecture (MDA) [4] is an approach to the system development life cycle, supported by models, from conception, throughout design, construction, deployment, operation and maintenance. The term architecture means the system specification, which details the system composition of parts and connectors, as well as the rules for the interactions among parts using the connectors. The MDA specification defines particular uses of certain types of models, their relationships, and how they can be built [5].

MDA is anchored in the idea of separation of concerns. This means separating the specification of a system from the details by which it uses the platform where is implemented. Through MDA one can specify a system independently of the platform that supports it, transform the system specification into another model suitable for that particular platform.

A relevant concept in MDA is the viewpoint. A viewpoint is an abstraction or simplification of a system, using a partial set of concepts and rules, and focusing so on a particular perspective of the system. On the other hand, a view is a representation of a system from the perspective of a chosen viewpoint. The Model-Driven Architecture specification defines three viewpoints on a system: a computation independent viewpoint, a platform independent viewpoint, and a platform specific viewpoint.

The Computation Independent Model (CIM) is a view of a system that does not show details of the structure of systems. It is considered as a domain model since it addresses the concepts, and their relationships, that are familiar to the domain's practitioners. The CIM bridges the gap between experts from the domain, knowledgeable of requirements, and the experts of design and construction of the artifacts that provide fulfillment of domain's requirements. CIM can also be considered as an abstract syntax of a language which vocabulary are the terms of the domain.

The Platform Independent Model (PIM) is a view of a system independent of the set of subsystems and technologies that provide a coherent set of functionalities, without concern of how it is provided by the platform. A PIM exhibits a specified degree of platform independence to be suitable for use with a number of different platforms of similar type, and the quality of platform independence, models should exhibit.

A Platform Specific Model (PSM) is a view of a system that combines the specifications in the PIM with the details of how the system uses a particular type of platform. A platform model provides the set of technical concepts, representing the different kinds of parts that make up a platform and the services provided by that platform. Is also part of the platform model's definition, to be used in a platform specific model, concepts representing the different kinds of elements for specifying the use of the platform by an application. The system is the composition of one or more applications on one or more platforms.

Model transformation [6], in the context of MDA, is the conversion process of one model into another model of the same system. The result of the transformation is a model specific to a particular platform, originated from a platform independent model.

As well as the present work applies the MDA paradigm to risk management and information security context, several other works have also applied MDA to other contexts, namely the following: process modeling [7, 8], service level management [9], ontology [10], software engineering [5], and industrial applications [11].

3 Modeling Risk Management and Information Security

In this section, we describe the two related models of Risk Management and Information Security. These interrelated domains were modeled according to the concepts described in ISO 31000:2009 [1] and ISO/IEC 27001 [3] standards.

The requirements for risk management and information security systems were modeled at higher level of abstraction of MDA, the CIM layer. Such models are independent of how the system will be implemented and hides the details on which implementation will be made.

The CIM is represented in a UML model [12] (Figure 1) that consolidates viewpoints from the several participants in the information security requirements definition, namely the concerns of, to name a few, the information security manager, information security committee, risk owners and asset owners.

3.1 Risk Management CIM model

In this section we describe a model for risk management. The model has, as central concept, *risk (management) architecture*, depicted at the center of the class diagram in Fig. 1.

It is assumed that the proposed model can be specialized to other disciplines, such *as information security*. The proposed model, following the ISO 31000:2009 standard, intends also to be applicable to other domains for which risk management is important, such as in the enterprise context, functional areas such as finance, in the business continuity endeavor, in time-delimited projects, healthcare or regarding safety issues. Therefore, the *risk entity*, the target of the risk assessment, can be the whole or part of an organization, a particular process, project, or product.

The concept of *risk* is linked to uncertainty and can be quantified as a positive or negative deviation from an expected *objective*, irrespective of which functional or domain area, as well as the organizational level it is defined. The profile of each risk is better characterized by linking it to the events that may happen, their consequences and the *likelihood* of the occurrence. The lack of information regarding the event occurrence, its consequence, or likelihood, is what drives to the state of uncertainty that underlies risk.

Risk architecture is a concept that includes the set of performed activities coordinated in order to direct and control the risk. For risk management accomplishment a *framework* must be implemented. The framework includes a set of plans, relationships, accountabilities, resources, processes and activities that provide the *policy* and *objectives* to manage risk. The risk management policy addresses the aims and strategy of the organization regarding risk management. The framework should not be implemented separately from the strategic and operational policies and practices of an organization. On the contrary the framework should be embedded within the actual practices of the organization. The framework should also drive the design, implementation, monitoring, reviewing and continually improving of organization's risk management.

The processes for tackling risks (aka risk management process) can be detailed in sequences of procedures, activities, practices, and responsibilities. The inherent activities can be classified as *communication and consultation*, *contextualization*, *assessment* (identification, analysis, and evaluation), *treatment*, *monitoring* and *reviewing* of risks.

The risk analysis is the process to comprehend the nature of risk and to determine the level of risk, which includes risk estimation. The terms of reference against which the significance of a risk is evaluated, based on organizational objectives, and external and internal context, is called risk criteria. The risk evaluation on the other hand, is the process of comparing the results of risk analysis with *risk criteria* to determine whether the risk and/or its magnitude is acceptable or tolerable. The process to modify risk is called risk treatment (e.g. risk mitigation), which can involve one or more of the following actions: removing the risk source; changing the likelihood; changing the consequences; avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; taking or increasing risk in order to pursue an opportunity; sharing the risk with another party or parties; retaining the risk by informed decision.

Monitoring is the continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected. Reviewing is the activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. Monitoring and Reviewing can be applied to the framework, processes, risks, or controls.

Each risk should have an assigned *owner* (stakeholder), i.e. a person or entity accountable for the risk and with authority to manage it.

The risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs. Risk identification involves the identification of risk *sources* of potential *events* and their *consequences*. A risk source is an element which alone or in combination has the intrinsic potential to give rise to risk. An event, on the other hand, is the occurrence or change of a particular set of circumstances. An event can be one or more occurrences, with several causes, or can consist of something not happening. An event can also have a range of outcomes or consequences affecting objectives. Consequences can be expressed qualitatively or quantitatively, be certain or uncertain and can have positive or negative effects on objectives. A *residual risk* is a risk remaining after risk treatment. The *risk profile* is the description of any set of risks.

The magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood is called the *level of risk*. Likelihood is the chance of something happening.

A *control* intends usually to be a measure for risk modification. Controls may include any process, policy, device, practice, or other actions which modify risk. Some mechanisms of risk control are: *liability transfer*, *indemnification*, *mitigation*, and *retention* [13].

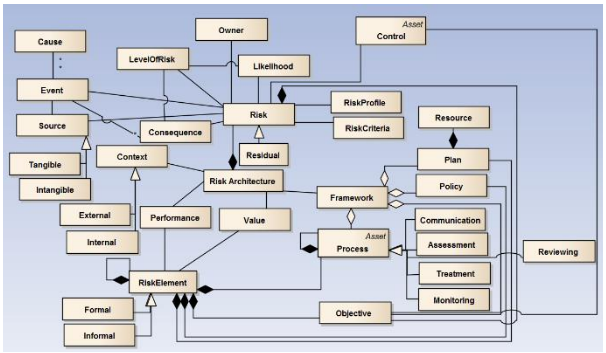

Fig. 1. A CIM model for risk management.

The model in Fig. 1 represents the concepts the above mentioned and their relationships regarding risk management systems.

3.2 Information Security CIM model

The viewpoint of the CIM model for the information security system is depicted in Fig. 2. In this model the term *asset* comes from the financial area, since it is considered an element of value for the organization, and therefore, needs adequate protection. So, an asset is defined as an element that is part of processes (denoted by the composition symbol near the process class), including the process itself (denoted by the inheritance symbol near the asset class), that manipulates the information, the information itself (either in physical or electronic support), the container in which the information is stored, the equipment in which the information is handled, transported, and made available.

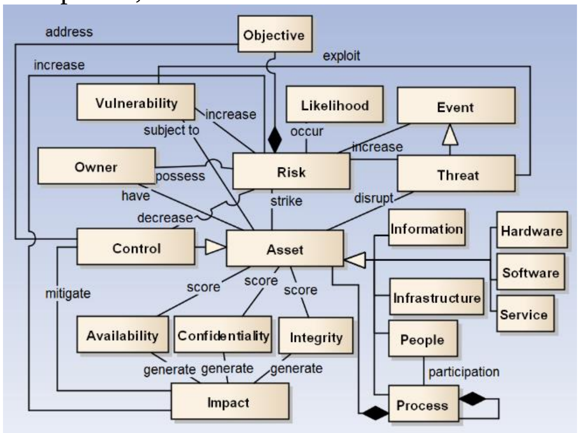

Fig. 2. A CIM model for Information Security.

As asset are also classified (denoted by the *is-a* relationship near the asset class): the hardware (e.g. laptops, servers, printers, and mobile phones); software (commercial or open source); infrastructure (e.g. buildings, offices, and air conditioning); people (e.g. employees, managers); and service providers (e.g. legal services, cleaning services, communications, and maintenance). For each asset, there is mandatory information to be collected, namely the legal, contractual or business requirements applicable to the asset, as well as the asset level of classification regarding information.

There are several ways of categorizing assets to facilitate their evaluation and treatment. By this way, it becomes easier to identify the boundaries of each group, given their specificity, and the qualitative benefit of security activities. With the identification of all the valuable assets associated with the information life cycle of the organization, ends the first step of risk assessment.

After assets identification, their owners are identified. They are persons, or the organizational units responsible for each asset life cycle (depicted as the association have between asset and owner classes). Also identified are the risks' owners, as providers of the means for asset protection (depicted as the possess association between risk and owner classes), as well as the risks' asset (depicted as the strike association between risk and asset).

The adverse impact of a security event on an asset is described in terms of loss or degradation of one of any combination of the three information security pillars: confidentiality, integrity, and availability (depicted as the score associations between asset, confidentiality, integrity, and availability classes). The asset evaluation process identifies how the categories of assets can be affected in each of those security pillars.

The categories of assets whose evaluation is greater than or equal to some specified threshold should be a candidate for risk assessment. The remaining categories of assets could be reviewed in the next revaluation.

The identification of risks and threats should be based on the organization's background, empirical knowledge, security weaknesses or the threat catalog available in ISO 27005 [14]. Risks or threats should be found for each category of assets. Each threat vs. vulnerability pair must correspond to an identified risk (depicted as the exploit association between threat and vulnerability classes). Vulnerability (e.g. lack of antivirus software) means the weakness in an asset that can be exploited by a threat (e.g. a virus attack). For each found risk a risk owner must be identified.

The adverse impact of a security breach should be evaluated in terms of loss of any combination of the information security pillars: confidentiality, integrity, and availability (depicted as the generate associations between the classes impact, confidentiality, integrity, and availability).

It should also be determined the likelihood of occurrence of vulnerabilities exploitation (likelihood of occurrence of identified risks). A level of likelihood must be determined for each risk (depicted as the association occurs between risk and likelihood classes).

A survey of active controls should be performed for each category of information assets in the context of each risk or pair, threat vs. vulnerability. Existing active and/or planned controls in the organization, to address the identified risks, should be verified. The identification of existing controls avoids unnecessary work and costs with possible duplication of controls. Controls that are not appropriate and can lead to vulnerabilities should also be identified.

The controls' objectives must be identified for each priority risk (depicted as the association address between control and objective classes). The appropriate controls must be selected to achieve the established objectives. The selection of controls should be based on the ISO 27001 Annex, but others sources of control may also be selected.

A cost estimation must be made for each identified control. The risk management team should propose the approach to identified risks and determine whether they will be accepted, reduced, transferred or avoided. This approach should be decided jointly by risk owners and managers.

3.3 Rules in CIM models

The above models represent part of the abstract syntax of risk management and information security systems. However, there are other important aspects of the risk management and information security, not depicted in the graphical representation: the rules that the risk management and information security systems must verify. So, the CIM must also incorporate the definition of rules that risk management and information security systems must comply with. Therefore, another important part of this work was the implementation of rules in the ISO 31000:2009 [1] and ISO/IEC 27001 [3] standards to be used to validate the conformance of actual risk management and information security systems.

For implementing formally the rules, OCL [15] was used. OCL is a declarative and predicate logic like language that supplements the UML and is used to implement rules in models by means of invariants. A formal language, as the OCL, can contribute for rigorously expressing well-formedness rules, which are hard to convey by graphical notations. With OCL we were able to improve the semantics of the CIM model.

Using the OCL textual notation, the specification of actual risk management and information security systems can be verified to determine the compliance of their properties regarding the ISO 31000:2009 [1] and ISO/IEC 27001 [3] set of standards. The rules' verification consists in applying a sequence of invariants to the specifications of a new risk management or information security systems system for checking their truthiness. With this approach, an actual system is then, amenable to be more rigorously checked and analyzed, through syntactic and well-formedness validations.

For the validation process an automatic tool, the USE (UML-based Specification Environment) [16], was used.

The CIM model, containing the rules for interpretation that all risk management or information security systems must conform, allows the validation of the PIM of a specific system. The PIM can also be loaded as a script to USE tool, which then checks the specific system (PIM) regarding the ISO 31000:2009 [1] and ISO/IEC 27001 [3] set of standards conformance. The non-conformities regarding the rules that are part of the CIM are marked as invariants violations, which must be corrected.

4 Conclusion

Information as a key asset to today's organizations must be protected from increasing threats. Implementing risk management and information security systems compliant with ISO 31000:2009 [1] and ISO/IEC 27001 [3] set of standards is the first step to ensuring confidentiality, integrity, and availability of the information.

This work followed an MDA approach on the implementation of risk management and information security systems. Since the models are at a high level of abstraction, this approach contributes for bridging the gap within the information security community between domain analysts, who work with security at a domain level (CIM), and security implementers, who analyze the same issues at an architectural and design levels (PIM).

Future work intends to extend risk management and information security models in order to include the dynamic perspective of information security, and also conduct empirical studies for assessing the usability and efficacy of the MDA approach in the risk management and information security domains.

References:

[1] ISO/IEC, "31010:2009, Risk management – Risk assessment techniques," 2009.

[2] A. Calder and S. Watkins, IT Governance: An International Guide to Data Security and ISO27001/ISO27002, Kogan Page, 2015.

[3] ISO/IEC, “27001:2013 - Information security management systems,” Book 27001:2013 - Information security management systems, Series 27001:2013 - Information security management systems, 2013.

[4] OMG, Object Management Group, MDA Guide Version 1.0.1, 2003.

[5] O. Pastor and J. Molina, Model-Driven Architecture in Practice : A Software Production Environment Based on Conceptual Modeling, Springer-Verlag Berlin and Heidelberg GmbH & Co., 2010.

[6] T. Mens and P. Van Gorp, “A Taxonomy of Model Transformation,” Electronic Notes in Theoretical Computer Science, vol. 152, 2006, pp. 125-142; DOI http://dx.doi.org/10.1016/j.entcs.2005.10.021

[7] A. Correia, “Quality of Process Modeling Using BPMN: A Model-Driven Approach”, PhD Thesis, UNL-FCT, 2014.

[8] A. Correia and F. Brito e Abreu, “Adding preciseness to BPMN models,” Procedia Technology, vol. 5, 2012, pp. 407-417.

[9] A. Correia and F. Brito e Abreu, “Model-driven service level management,” Proc. IFIP International Conference on Autonomous Infrastructure, Management and Security, Springer Berlin Heidelberg, 2010, pp. 85-88.

[10] D. Ga, et al., Model driven architecture and ontology development, Springer Science & Business Media, 2006.

[11] S. Burmester, et al., “Model-Driven Development of Reconfigurable Mechatronic Systems with Mechatronic, UML,” Model Driven Architecture: European MDA Workshops: Foundations and Applications, MDAFA 2003 and MDAFA 2004, Twente, The Netherlands, June 26-27, 2003 and Linköping, Sweden, June 10-11, 2004. Revised Selected Papers, U. Aßmann, et al., eds., Springer Berlin Heidelberg, 2005, pp. 47-61.

[12] O.M.G. OMG, “UML - Unified Modeling Language Version 2.5,” 2015.

[13] B. Blakley, et al., “Information security is information risk management,” Book Information security is information risk management, Series Information security is information risk management, ed., ACM, 2001, pp. 97-104.

[14] ISO, “ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management”, 2011.

[15] OMG, The Object Management Group, “Object Constraint Language (OCL),” OMG Available Specification, vol. Version 2.0, 2006; DOI formal/06-05-01.

[16] M. Gogolla, et al., “System modeling with USE (UML-based Specification Environment),” Genie Logiciel, no. 85, 2008, pp. 57-58.