Manage Risks through the Enterprise Architecture

José Barateiro
LNEC, INESC-ID
jbarateiro@lnec.pt

Gonçalo Antunes
INESC-ID
goncalo.antunes@ist.utl.pt

José Borbinha
INESC-ID
jlb@ist.utl.pt

Abstract

The goal of Risk Management activities is to define prevention and control mechanisms to address the risks attached to specify activities and valuable assets. Many Risk Management efforts operate in silos with narrowly focused, functionally driven, and disjointed activities. That fact leads to a fragmented view of risks, where each activity uses its own language, customs and metrics. The lack of interconnection and holistic view of risks limits an organization-wide perception of risks, where interdependent risks are not anticipated, controlled or managed. In order to address the Risk Management interoperability and standardization issues, this paper proposes an alignment between Risk Management, Governance and Enterprise Architecture activities, providing a systematic support to map and trace identified risks to enterprise artifacts modeled within the Enterprise Architecture, supporting the overall strategy of any organization. We discuss the main relationships between Risk Management and Enterprise Architecture and propose an architecture to integrate risks concerns into the overall organization environment.

1. Introduction

Risk Management (RM) is a continuously developing arena whose ultimate goal is to define prevention and control mechanisms to address the risks attached to specific activities and valuable assets. The early identification of potential problems allows the creation of plans to reduce their potential adverse impact [1]. A RM process describes a set of systematic activities to support the proactive identification and mitigation of risks within a specific environment.

Depending on the knowledge area, several definitions of risk can be found in the literature. For instance, in [2] risk is defined as: "An undesirable outcome that poses a threat to the achievement of some objective. A process risk threatens the schedule or cost of a process; a product risk is a risk that may mean that some of the system requirements may not be achieved."

Similarly, the ISO Guide 73:2009 [3] defines risk as: "...the combination of the probability of an event (threat[1]) and its consequences when exploiting any vulnerability[2]".

Risk always exists, whether or not it is detected or recognized by an organization. Several areas involve risks that should be treated to provide significant benefits to an organization, like business risks, market risks, credit risks, operational risks, IT risks, engineering, etc. Thus, RM strategies vary from generic approaches, project management, IT (including information security), safety engineering, etc. Highly specific areas, like aviation or banking, are more focused on analytical methods to assess and quantify risks, rather than processes and methodologies to manage the overall risk environment.

Despite the fact that different communities use different terminology and phrasing to define risks, they share the main basic concepts, which are illustrated in Figure 1.

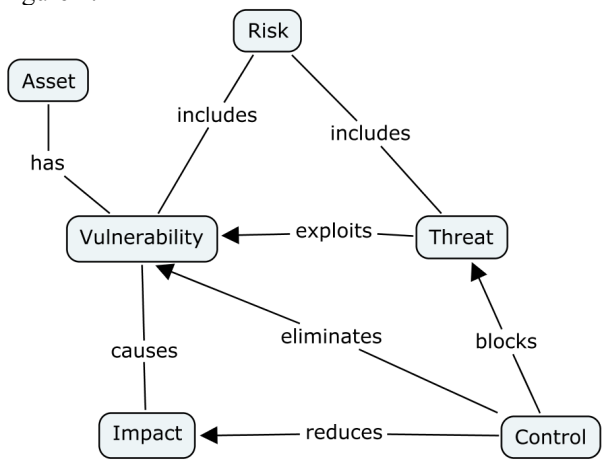

Figure 1. Risk Management Concepts

[1] Threat is any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service [3].

[2] Vulnerability is the existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved [3].

978-0-7695-4525-7/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2012.419

A risk exists when a threat with the potential to cause loss or harm occurs and is able to exploit a vulnerability/weakness associated with an asset that has a value to be protected. The type of assets depends on the nature of the organization, but might include physical entities (e.g., person, office), information entities and processes. When the vulnerability is exploited, it causes an impact on the achievement of the organization objectives. The goal of RM is to manage risks by defining a set of adequate controls to block threats, eliminate vulnerabilities or reduce the impact of the risk occurrence.

Analyzing and modeling risks is one of the most critical task in the overall process of RM. Traditional approaches, such as Fault Tree Analysis, Event Tree Analysis, Failure Mode Effect and Criticality Analysis are commonly used to model risks in the safety community [9,10]. However, these approaches are not suitable to address the imminent risks that today's organizations face at multiple levels (both internally and externally).

Several models have been proposed to address risks at the organizational level, integrating the different views of the related stakeholders, such as the COSO Enterprise RM framework (see Section 2), KAOS [11], GBRM [12] and the Tropos Goal Risk Model [13]. Risks at the organizational level are covered by Enterprise Risk Management (ERM), which provides a framework to manage the uncertainty and the associated risks and opportunities in the global scope of an organization. Thus, ERM should be seen as an enabler to the organizations, being impossible to operate on silos. In fact, ERM is part of the corporate governance, providing risk information to the board of directors and audit committees. It is also related to the performance management by providing risk adjustment metrics, with internal control, and with external audit firms. This increases the requirement to be able to exchange risk information, supporting the interoperability[3] of risk information.

RM activities must be aligned with the business processes of the organization [14]. When organization business processes and strategic planning are aligned with proactive RM activities, a well-defined path and strategy to attain business value is achieved. However, no known business processes have the capability to formally define the sources and dependencies of risks [15]. Moreover, obtaining value through risk assessment can only be achieved through appropriate reporting and communication mechanisms. Due to a complete view of organization's risks, overall risk information becomes visible to executives and management boards, making it possible to incorporate this information to strategic and operational planning.

Furthermore, as computer systems quickly spread into organizations' processes that have a human, social and organizational purpose; it is crucial to have a holistic view of the overall sociotechnical system [16]. Due to the interactions and dependencies between different layers of the sociotechnical system, the implications that result from a problem in one of the layers are increased. As a consequence, software components must be trustworthy, being available when required, and operating correctly without producing undesired effects. The trustworthy degree of a computer system is usually known as its dependability [17], which can be seen as a set of protection requirements to protect systems against abnormal events (e.g., internal failures, attacks) [2]. In order to define adequate protection requirements, it is required to understand the risks that can affect the system and its environment. A risk-driven approach is widely used to understand the events that could cause damage and that are likely to occur. In complex dependable systems with interactions and dependencies between different components, the holistic view and sharing of risk information becomes an important tool to achieve the most suitable protection requirements.

Indeed, one of the main problems of RM is the fact that several efforts operate in silos with narrowly focused, functionally driven, and disjointed activities [14]. This leads to a fragmented view of risks, each using their own language, customs and metrics. The lack of interconnection and holistic view of risks hampers an organization-wide view of risks, where interdependent risks are not anticipated, controlled or managed. On the other hand, there is an increasing requirement to exchange risk and control information between organizations and external audit firms. Mapping risk and control information, both internally and to external organizations is highly expensive and inefficient. The lack of interoperability mechanisms between applications used to support different techniques also impedes the analysis of interrelated risks.

This paper proposes an alignment between RM, Governance and Enterprise Architecture (EA) activities, in order to provide a systematic support to map and trace identified risks to artifacts modeled within an EA, supporting the overall strategy of any organization. We analyze the relationships between RM and EA activities and propose a solution to manage the risk information in an integrated and holistic way.

The remainder of this paper is organized as follows. First, in Section 2 we describe the related

[3] As defined by the Institute of Electrical and Electronics Engineers (IEEE), interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged [8].

work in the areas of IT Governance, RM and EA. Section 3 shows the proposed approach to address risks through the EA, while Section 4 details the relation between EA and RM processes. Section 5 details the architecture view for the management of risk information. Finally, Section 6 presents the main conclusions of this work.

2. Related work

IT Governance

IT Governance encompasses "the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives" [27].

The key governance framework COBIT organizes activities into a well-defined process model and identifies which resources can be leveraged to achieve specified objectives. It aims to ensure alignment between technology and business requirements by making performance against measures transparent and defining control objectives to govern processes. COBIT provides a controlled process model organized in four domains: Plan and Organize; Acquire and Implement; Deliver and Support; Monitor and Evaluate. COBIT relates all processes to each other through input and output dependencies and models the relevance of each process in supporting a number of information criteria (Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance, and Reliability). Finally, COBIT includes a maturity model based on the CMMI [1] and ISO 15504 [6], a capability model developed to integrate practices, methods and maturity models for different disciplines in a process improvement approach. The main goal is to help organizations to manage and control nowadays' complex development and maintenance processes, providing best practices that address development activities applied to products and services.

Risk Management

RM frameworks are especially concerned with the definition of a set of principles and foundations to guide the design and implementation of RM processes in any type of organization. Since they are not focused on any specific area of implementation, it is not possible to find any recommendation about adequate methods to execute within the RM process or even a previous knowledge base with common risks and suitable treatment plans for the identified risks.

The ISO 31000:2009 RM standard [4] is based on the principle that RM is a process operating at different levels, as shown in Figure 2. The RM process is characterized by the combination of policies and procedures applied to the activities of establishing the context, assessing (identifying, analyzing and evaluating), treating, communicating, consulting, monitoring and reviewing the risks.

First, defining the context is crucial to identify strategic objectives and define criteria (both internal and external parameters) to determine which consequences are acceptable to this specific context. Second, today's organizations are continuously exposed to several threats and vulnerabilities that may affect their normal behavior. The identification recognizes the existence of risks; the analysis examines the nature and severity of the identified risks; and the evaluation compares the severity of risks with the defined risk criteria, to decide if the risks are acceptable, tolerable or define the appropriate techniques/controls to handle them.

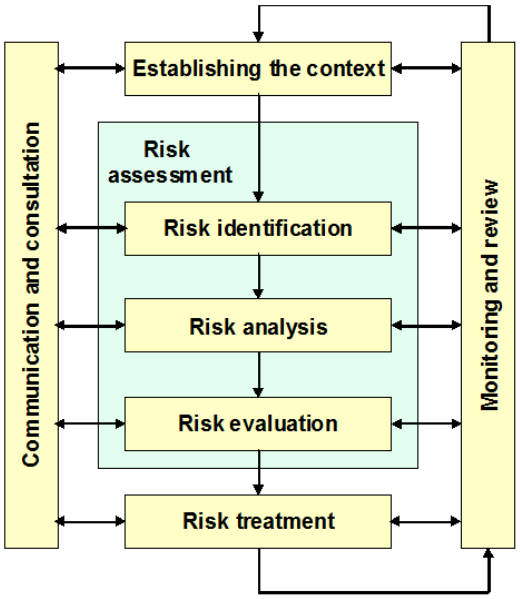

Figure 2. Risk Management Process

The identification of threats, vulnerabilities and risks is based on events that may affect the achievement of the goals identified in the first phase. After that, the risk analysis and evaluation estimates the likelihood and impact of risks to the strategic goals, in order to be able to decide on the appropriate techniques to handle these risks (Treat Risks).

The RM process requires a continuous monitor and review activity to audit the behavior of the whole environment allowing, for instance, the identification of changes in risks, or the suitability of implemented risk treatment procedures and activities. Finally, the communication and consultation activities are crucial to engage and dialog with stakeholders.

The ISO/IEC 31010:2009 - Risk Assessment Techniques [5] surveys 31 techniques to perform risk assessment. It supports the ISO 31000:2009, by describing risk assessment techniques, and showing how they can be applied to each step of the risk assessment process as follows: (*i*) risk identification; (*ii*) risk analysis - consequence analysis; (*iii*) risk analysis - qualitative, semi-quantitative or quantitative probability estimation; (*iv*) risk analysis - assessing the effectiveness of any existing controls; (*v*) risk analysis estimating the level of risk; and (*vi*) risk evaluation.

Enterprise Risk Management (ERM) is the process of identifying and analyzing risks, from an integrated and organization-wide perspective [18].

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) view of ERM is that "Every entity exists to provide value for its stakeholders" [19]. In fact, all entities can face several types of uncertainty, raising a challenge to the management on how to deal with such uncertainty in a way that maximizes the values of those entities for the interested stakeholders.

In 2004, COSO issued the COSO ERM Framework [19] to provide a common accepted model for evaluating and aligning effective enterprise-wide approaches to RM. This framework defines essential ERM components; discusses key ERM principles and concepts, and suggests a common ERM language.

Figure 3. COSO ERM Framework

As shown in Figure 3, the COSO ERM Framework analyzes ERM from three different dimensions: Objectives, Organization (and organization units) and components of ERM.

Within the context of an organization vision, management establishes objectives for several levels. The COSO ERM framework organizes objectives in four categories:

- Strategic: high-level goals to support the organization's mission.
- Operations: effective use of the organization operational resources.
- Reporting: reliability of reporting (both for internal and external stakeholders).
- Compliance: compliance with applicable law and regulations.

The proposed categories might overlap, since a specific objective can fall into more than one category, but support the focus on distinct issues of ERM.

The organization dimension considers ERM activities at all levels of the organizational architecture (e.g., Organization-level, Division, and Business Unit).

Finally, the framework is composed by eight interrelated components:

- Internal Environment - encompasses the tone of an organization, and establishes the basis for how RM is viewed and addressed.
- Objective Setting - the definition of objectives is required to allow the identification of potential events affecting their achievement.
- Event Identification - identification of events that may affect the achievement of objectives. Events that may cause a negative impact represent risks, while events that may have a positive impact represent opportunities.
- Risk Assessment - understand the extent of incidents, analyzing their likelihood and impact. It is used to assess risks and also to measure the related objectives. Assessment can be qualitative or quantitative.
- Risk Response - identifies and evaluates potential responses (avoiding, accepting, reducing or sharing) to risk.
- Control Activities - set of policies and procedures to ensure that risk responses are effectively carried out.
- Information and Communication - relevant information concerning risks is captured and communicated to stakeholders to carry out their responsibilities.
- Monitoring - the effectiveness of other ERM components is monitored through continuous monitoring activities or separate evaluations.

Note that ERM is not a series of independent processes, but a multidimensional and iterative discipline where each component can influence another.

	DATA What	**FUNCTION** How	**NETWORK** Where	**PEOPLE** Who	**TIME** When	**MOTIVATION** Why
SCOPE (contextual)	List of things important in the business	List of business processes	List of business locations	List of important organizations	List of events	List of business goals and strategies
BUSINESS (business model)	Conceptual data/object model	Business process model	Business logistics system	Work flow model	Master schedule	Business plan
SYSTEM (logical model)	Logical data model	System architecture model	Distributed systems architecture	Human interface architecture	Processing structure	Business rule model
TECHNOLOGY (physical model)	Physical data/class model	Technology design model	Technology architecture	Presentation architecture	Control structure	Rule design
COMPONENTS (detailed)	Data definition	Program	Network architecture	Security architecture	Timing definition	Rule specification
INSTANCES (functioning enterprise)	Usable data	Working function	Usable network	Functioning organization	Implemented schedule	Working strategy

Figure 4. The Zachman framework

Enterprise Architecture

Architectural descriptions provide rigorous descriptions of complex systems with diverse concerns, and are a recommended approach to tackle the dynamic and increasing complexity of those systems. According to the IEEE Std. 1471-2000, which has also become ISO/IEC 42010:2007, architecture is "the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution" [7]. It considers that a system has a mission and inhabits an environment which influences it. It also has one or more stakeholders that have concerns regarding the system and its mission. Concerns are "those interests that pertain to the system's development, its operation, or any other aspects that are critical or otherwise important to one or more stakeholders".

A system has an architecture described by an architecture description which includes a rationale for the architecture. The architecture description is also related with the stakeholders of the system and deals with several views according to the viewpoints of the stakeholder. This includes functional and non-functional aspects of stakeholders' concerns.

Accurate architecture descriptions provide a "complete picture" of the overall system. However, any system (especially a complex system made of software, people, technology, data and processes) is continuously subject to changes, usually driven by the evolution of the system environment [20].

Enterprise Architecture is a holistic approach to systems architecture with the purpose of modeling the role of information systems and technology in the organization, aligning enterprise-wide concepts and information systems with business processes and information. It supports planning for sustainable change and provides self-awareness to the organization [21].

The Zachman framework is a "way of defining an enterprise's systems architecture" with the purpose of "giving a holistic view of the enterprise which is being modeled" [22]. It can also be described as a "classification theory about the nature of an enterprise" and the kinds of entities that exist within. As shown in Figure 4, the Zachman framework presents itself as a table where each cell can be related to the set of models, principles, services and standards needed to address the concerns of a specific stakeholder. The rows depict different viewpoints of the organization (*Scope*, *Business*, *System*, *Technology*, *Components*, and *Instances*), and the columns express different perspectives on each of the viewpoints (*Data*, *Function*, *Network*, *People*, *Time*, *Motivation*). Due to its visually appealing nature almost resembling a “periodic table of the elements” of descriptive representations of the organization, it is very useful in analyzing the scope of specific models and frameworks, and in reconciling potentially conflicting viewpoints.

The Open Group Architecture Framework (TOGAF) [23] provides methods and tools to support architecture development. It comprises seven modules which can be partly used independently of each other. The core of TOGAF is the Architecture Development Method (ADM), which consists of a cyclical process divided in nine phases as shown in Figure 5.

After a *preliminary* phase in which the context, relevant guidelines, standards, and goals are identified, the main process begins with the elaboration of an *architecture vision* and the principles that should guide the architecture work. This *architecture vision* phase provides the basis for developing the *business architecture*, *information systems architecture*, and

technology architecture. On this basis, solutions are developed (*opportunities and solutions* phase), and migration and implementation are planned and governed (*migration planning* and *implementation governance* phases).

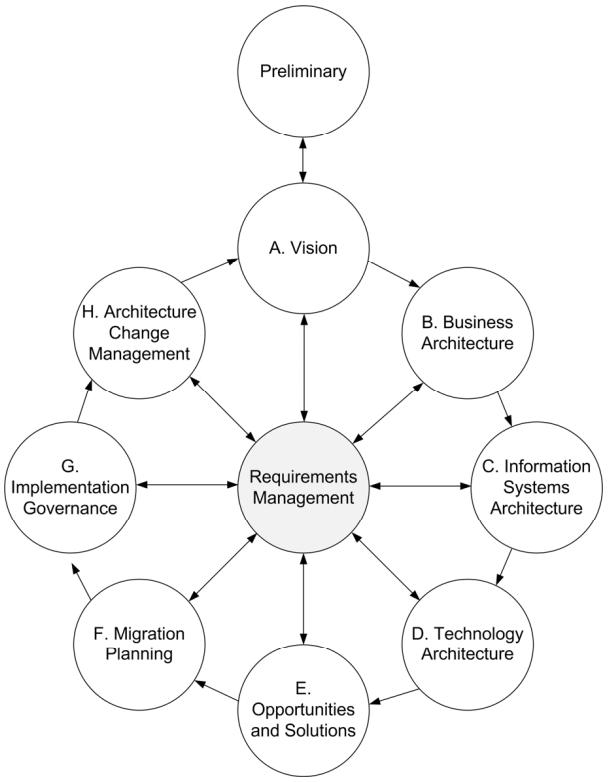

Figure 5. TOGAF Architecture Development Method (ADM)

Finally, the *architecture change management* phase ensures that the architecture continues to be fit for purpose. All of the phases are executed concurrently with a *Requirements Management* activity, which drives the other phases. The ADM can be adapted for various purposes, and in more complex situations, the architecture can be scoped and partitioned so that several architectures can be developed and later integrated using an instance of the ADM to develop each one of them.

3. Approach

This paper proposes an alignment between Risk Management (RM), Governance and Enterprise Architecture (EA) activities. The main rational for this proposal is to provide a systematic support to map and trace identified risks to enterprise artifacts modeled within an EA, supporting the overall strategy of any organization. Figure 6 represents the overall approach.

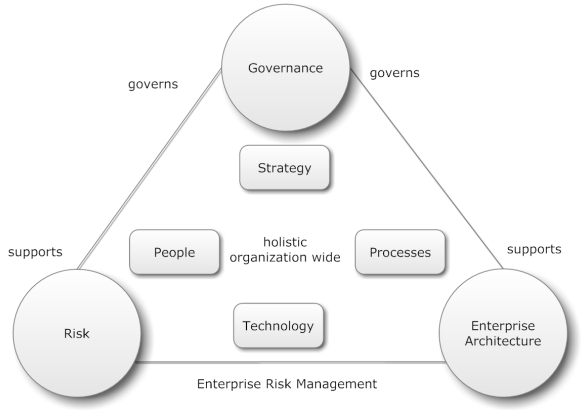

Figure 6. Integrating Risk Management into the organization

In fact, Governance processes intend to ensure the comprehensive control when moving from strategic planning to operative implementation. This task demands orientation and transparency that can be supported by EA processes. Indeed, EA can be used to reveal deficiencies, show complex interactions between strategies, business processes, services and infrastructure, providing a foundation for complex analysis (either by Governance or Risk Management activities). We propose an integrated view of Governance, Risk and EA to support organizations to be efficient, effective and reliable. In other words, decision making must be able to do the right things in the right way with a controlled risk.

Organizations can be described in terms of their architecture. The existence of a description of EA artifacts (e.g., data models, business models, strategies, infrastructure plans, hardware, functions, organizational structure, etc) denotes awareness of organization concerning its architecture. Like in buildings, the architecture always exist, either it is recognized, planned and supported by accurate models, but also in scenarios where EA is not recognized by organizations.

When we consider the relation between Governance and EA, EA provides transparent information as a basis for decision making and control activities (Governance). However, this should not be seen as a static relation, since it is also about the continuous provision of updated and accurate information that enables governance, bridging the gap between strategic planning and real operations (strategic alignment).

The interaction between Governance and Risk is already recognized by the broader area of Governance, Risk and Compliance (GRC). In fact, the increasing spread of regulations like Basel II and the Sarbanes-Oxley Act, along with the ultimate series of global economic and financial events, raised the awareness to

Table 1. Analysis of Risk Management and Enterprise Architecture Processes

		ISO 31000						
		Establish the context	Identify Risks	Analyze Risks	Evaluate Risks	Treat Risks	Monitor and Review	Communicate and consult
TOGAF-ADM	Requirements Management	M	M	M	M	M	M	M
	Preliminary	M						M
	Vision	M						M
	Business Architecture		EA2RM	EA2RM	EA2RM			M
	Information Systems Architecture		EA2RM	EA2RM	EA2RM			M
	Technology Architecture		EA2RM	EA2RM	EA2RM			M
	Opportunities and Solutions					M		M
	Migration Planning					RM2EA		M
	Implementation Governance					RM2EA		M
	Architecture Change Management	M	EA2RM				M	M

M: Mutual influence; EA2RM: EA influences RM; RM2EA: RM influences EA

effectively address the GRC activities of today's organizations [25]. The concepts involved in GRC are not new, but are traditionally addressed as separate concerns inside the organizations. However, these concepts share a set of knowledge, methodology and processes, which allows an optimal and holistic view where GRC activities are addressed in an integrated way to improve decision making, strategy setting and performance. This avoids conflicts, overlaps and gaps between the GRC activities.

Finally, we also propose a connection between Risk and Enterprise Architecture (detailed in Section 4). In fact, risk activities are usually performed in silos and without a clear mapping between risks and potentially affected organization components. We propose to extend risk activities to map risks to EA components, in a way that it is possible to analyze the spreading of risks that can directly affect only one component but contaminate a larger set of valuable assets. On the other hand, updates to the EA will also be reflected in the risk information.

In order to share information between Governance, Risk and EA, providing a common understanding and holistic view of the shared information, we propose to operate on the middle of the Governance, Risk and EA triangle.

4. Enterprise Architecture and Risk Management

This Section details the relationships between EA and RM. Table 1 shows the mappings between the TOGAF-ADM for EA and the ISO 31000 RM process.

First, establishing the RM internal and external context involves the perception of key values for stakeholders, trends, organizational culture, legal environment, etc., which are also addressed by the three EA phases: *requirements management*, when defining/refining the overall requirements; *preliminary*, when defining the main goals, constraints and principles; and *vision*, when drafting an initial model to represent the overall organization vision on the architecture. In this case, the connection between EA and RM is mutual, since both processes can be used as inputs for the other process (e.g., results from a RM *establish the context* process can be used when establishing the EA *vision*).

Identifying risks through a systematic analysis approach can be done using the business, information systems and technology architectures, to identify vulnerabilities in current information entities, processes, actors or technology infrastructure, against threats driven from the specified requirements and context. Similarly, *risk analysis* (e.g., likelihood estimation, consequences) and *evaluation* (e.g., identify options, establish priorities) can also make use of the rigorous descriptions provided by the EA. For instance, it is possible to analyze the spread of exploiting a vulnerability in a specific technology component (e.g., affected business processes, information entities, stakeholders, etc.).

The risk treatment options and plans provided by the RM *treat risks* process can be used by the EA *opportunities and solutions* phase to establish an initial implementation/migration plan for the overall architecture (this can include the redesign of business processes, replacement of hardware components, etc.). In the opposite way, the seeking for solutions in the EA process can also provide important inputs to evaluate potential risk treatment options. This can be done in a "including way" (this approach can be used to reduced a specific set of risks), but also in an "excluding way"

(the treatment option cannot be used because it violates requirements or does not conform to specific concerns within the EA.

Similarly to the relation between risk treatment and opportunities and solutions, the results from the *treat risks* phase can also be used by the *migration planning*, when defining the process to create, evolve and monitor the implementation to enable the realization of the architecture as established in the *opportunities and solutions* phase. With regard to the implementation governance we can consider that this phase is seen as a project management activity, which can involve a complete risk management process for this single purpose. However, limiting the context to the direct relations, the risk plans defined by the risk treatment phase of the RM process, will provide crucial information to define governance and management activities to realize the architecture, ensuring the conformance to the defined architecture, with a controlled risk.

The *architecture change management* phase intends to ensure that the architecture continues to be fit-for-purpose, assessing its performance and identifying changes to the framework and principles identified in the previous phases. This can act as a monitoring component that will be able to identify modifications in EA components. Since we track the risks against EA components, a modification can lead to a new risk or change the severity of previous identified risks, which is represented by the influence of this activity into the identification of risks. On the other hand, the monitoring nature of this phase is similar to the monitor and review process, where both activities can inform the other with updated information (the mapping between risks and EA components allows this bidirectional information flow). Also, the monitoring activities are strongly connected to the EA *Requirements Management* that requests information from other activities to update the conformance of the specified requirements with existing deployed solutions

Finally, since the goal of the RM *communicate and consult* process is to establish a communication channel with all the involved stakeholders, this activity crosses all the EA processes, as EA is organized from a high-level planning to the systems' implementation, where each phase is connected to specific stakeholders.

5. Solution Overview

In order to address the interoperability and standardization issues in RM and between RM and the related activities of Governance and EA, we propose a RM Framework, including a XML-based Domain Specific Language for RM (Risk-DL), supported by a formal definition of the RM concepts. The proposed framework is supported by an information system to manage the definition or risks. Moreover, the deployed solution is integrated with a Metadata Registry (MDR) to accommodate and map different representations of risks into the risk definition language.

The use of a MDR intends to ensure interoperability between different risk representations, as proposed by ISO/IEC 11179 [26], where an information system is responsible for managing and publishing descriptive information about resources (risk information). A MDR promotes interoperability by using a common reference model to register the descriptions of the data (semantic interoperability) and the context where it should be used (pragmatic interoperability), while registering version information about the data object (dynamic interoperability) and the corresponding relations (conceptual interoperability), whether related to relationships between different versions of the same or different data objects. This way, the syntactic representation of the *Risk-DL* language is irrelevant for the overall purpose of this solution.

The proposed solution also provides a set of decision support metrics to help in the definition of adequate risk treatment plans, and enable the analysis of the effectiveness of distinct treatment plans. This solution allows a holistic management of different categories of risks throughout the enterprise, providing an overall view of enterprise risks.

The architecture of the proposed solution is detailed in Figure 7. The *Operator* represents the *business worker* that is responsible to interact with the system. First, the *Operator* provides a *Risk Description* that is transformed into the *Risk-DL Specification* of these risks, using the *Risk Modeling* component. The transformation into the *Risk-DL Specification* is supported by the *MDR* component. This way, the architecture supports different versions of *Risk-DL*, as well as other risk representations[4]. The rational for this approach is based on the separation of concerns between the risk information and the services processing it.

The *Risk Analyzer* parses a *Risk-DL Specification* and generates an internal *Risk Representation* to be used and processed by the *Plan Generator*, which is responsible to produce options to manage risks (*Risk Plans*), based on previous knowledge stored in the *Risk Library*.

The *Risk Library* represents a risk knowledge base, locally storing validated risk information as, for

[4] In order to support different risk representations, both the risk representation and the respective transformation into the correspondent *Risk-DL* representation have to be specified in the MDR.

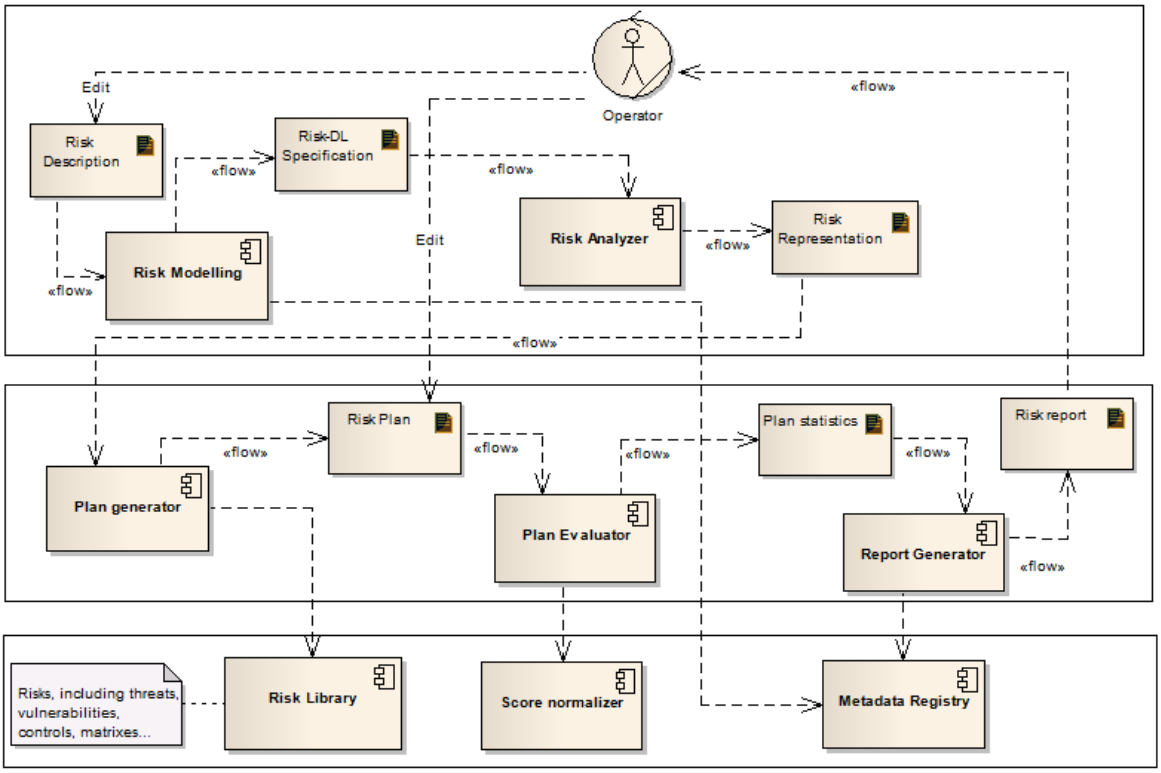

Figure 7. Architecture Overview

instance, risks used in previous scenarios, risk matrices, threats, vulnerabilities, assets, controls, plans, etc.

In order to support the complex decision of the most suitable risk treatment plan for a specific scenario, the *Plan Evaluator* produces a set of statistics that can be used to compare plans. When risks were defined according to different types of scores (quantitative, qualitative, semi-quantitative, or different scales), the *Risk Normalizer* is responsible to normalize scores, turning it possible to compare and rank risks defined using different methods.

Finally, the *Report Generator* produces *Risk reports* to support the decision on the optimal plan to apply. Also, risk information must be delivered to different stakeholders (with different concerns). Having this in consideration, the *Report Generator* is connected to the MDR to be able to provide different representations to view the risk information from the perspective of the concerns of every stakeholder.

Note that the proposed solution focuses on the risk dimension of the approach described in section 3. The relation to EA and Governance is expressed on the fact that *Risk-DL* maps risks to artifacts defined in the EA. Also, the interoperability supported by the way that risks are defined, allows the integration of risks delivered by different organization units (usually done in silos without any connection to other risks identified in organization), supporting a holistic view and integrated management of risks. Finally, the reporting mechanisms provide metrics and reports to support an effective decision making, based on risk and optional paths to deal with them.

6. Conclusions

Traditional RM efforts operate on silos, limiting the sharing of risk information and the achievement of an updated and organization-wide view of risks. Recently, there has been an effort on the area of ERM, but current solutions and frameworks are not aligned with recognized and well established EA frameworks, like the Zachman framework or TOGAF. In fact, EA descriptions provide a common way to model complex business systems, from the strategic level to implementation details.

This paper motivates the use of EA descriptions to represent risk information, allowing a better understanding on the value of assets on the components that can be affected from the manifestation of some risk. In fact, a risk that directly affects an EA component (e.g., a business process) will produce an impact on other components (e.g., other business processes, services, etc.). On the other hand, we discussed the main relationships between the TOGAF-ADM and the ISO 31000 RM process, which are prominent references on the scope of EA and RM, respectively. This analysis showed several connections between these processes, motivating a collaboration of

efforts to achieve the very same organization objectives.

Finally, this paper proposes a solution to achieve the holistic and common view of risks within an organization. This solution relies on the interoperability between risk tools (e.g., performing risk monitoring, evaluation) and EA descriptions, using an XML based language and a MDR to transform different risk representations into our solution. This way, the proposed solution is not limited to a specific set of tools, neither to a specific language to represent EA artifacts (e.g., UML, BPMN, BPEL, etc.).

Acknowledgments

This work was supported by FCT (INESC-ID multiannual funding) through the PIDDAC Program funds and by the projects SHAMAN and TIMBUS, partially funded by the EU under the FP7 contracts 216736 and 269940.

References

[1] Carnegie Mellon University, "Software Engineering Institute. Capability Maturity Model Integration for Development", Version 1.3, November, 2010.

[2] I, Sommerville, "Software Engineering (7th Edition)", Addison Wesley, 2004.

[3] International Standards Organization. "Risk Management -- Vocabulary" (ISO Guide 73:2009), 2009.

[4] International Standards Organization. "Risk Management -- Principles and guidelines" (ISO 31000:2009), 2009.

[5] International Standards Organization. "Risk Management – Risk assessment techniques" (ISO/IEC 31010:2009), 2009.

[6] International Standards Organization. "Information technology – Process assessment – Part 1: Concepts and vocabulary" (ISO/IEC 15504-1:2004), 2004.

[7] IEEE Standards Association. "IEEE Recommended Practice for Architectural Description for Software-Intensive Systems" (IEEE 1471:2000), 2004.

[8] IEEE Standards Association. "IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries", 1990.

[9] M. Stamatelatos, W. Vesely, J. Dugan, J. Fragola, J.Minarick and J. Railsback. "Fault Tree Handbook with Aerospace Applications", NASA, 2002.

[10] US Department of Defense. "DoD: Military Standard, Procedures for Performing a Failure Mode, Effects, and Critical Analysis", (MIL-STD-1692A), 1980.

[11] A. Dardenne, A. van Lamsweerde and S. Fickas. "Directed Requirements Acquisition", Science of Computer Programming (20), 1993, pp. 3-50.

[12] A. Anton. "Goal-Based Requirements Analysis", International Conference on Requirements Engineering, IEEE Computer Society, Washington DDC, USA, 1996.

[13] Y. Asnar and P. Giorgini. "Modelling Risk and Identifying Countermeasure in Organizations", Critical Information infrastructures Security, Springer Berlin / Heidelberg, 2006, pp. 55-66.

[14] S. Maziol. "Risk Management: Protect and Maximize Stakeholder Value", Oracle Governance, Risk, and Compliance, 2009.

[15] J. Lambert, R. Jennings and N. Joshi. "Process mapping techniques and organisational analysis: Lessons from sociotechnical system theory", Business Process Management Journal 1(8), 2002, pp. 42-52.

[16] S. Biazzo. "Integration of Risk Identification with Business Process Models", Systems Engineering 9(3), 2006, pp. 187-198.

[17] A. Avizienis, J.C. Laprie, B. Randell and C. Landwehr. "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE Trans. Dependable Secur. Comput. 1(1), IEEE Computer Society Press, 2004, pp. 11-33.

[18] The Institute of Internal Auditors "Managing Risk from the Mailroom to the Boardroom", Tone at the Top (18), IEEE Computer Society Press, 2003, pp. 11-33.

[19] Committee of Sponsoring Organizations of the Treadway Commission "Enterprise Risk Management - Integrated Framework", 2004.

[20] T. Mens, J. Magee and B. Rumpe "Evolving Software Architecture Descriptions of Critical Systems", Computer (43), IEEE Computer Society, Los Alamitos, CA, USA, 2010, pp. 42-48.

[21] P. Sousa, A. Caetano, A. Vasconcelos, C. Pereira and J. Tribolet "Enterprise Architecture Modeling with the Unified Modeling Language", Enterprise Modeling and Computing with UML, IGI Global, 2006.

[22] J. Zachman."A Framework for Information Systems Architecture", IBM Systems Journal 6(12), 1997, pp.276-292.

[23] The Open Group "TOGAF Version 9" Van Haren Publishing, 2009.

[24] US Department of Defense "DoD Architecture Framework, Version 2.0" Washington D.C., USA, 2009.

[25] M. Frigo and R. Anderson "A Strategic Framework for Governance, Risk, and Compliance" Strategic Finance 8(90), 2009.

[26] International Standards Organization. "Information technology – Metadata Registries (MDR)" (ISO/IEC 11179), 2005.

[27] IT Governance Institute. "COBIT 4.1. Framework". 2007