Proceedings of the Federated Conference on
Computer Science and Information Systems pp. 791–798

ISBN 978-83-60810-22-4

Integrated management of risk information

José Barateiro
INESC-ID, LNEC
Rua Alves Redol 9, 1000-029, Lisboa, Portugal
Email: jose.barateiro@ist.utl.pt

José Borbinha
INESC-ID
Rua Alves Redol 9, 1000-029, Lisboa, Portugal
Email: jlb@ist.utl.pt

***Abstract*—Today's competitive environment requires effective risk management activities to create prevention and control mechanisms to address the risks attached to specific activities and valuable assets. One of the main challenges in this area is concerned with the analysis and modeling of risks, which increases with the fact that current efforts tend to operate in silos with narrowly focused, functionally driven, and disjointed activities. This 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 and governance of any organization. We propose an architecture where risks are defined through a XML-based domain specific language, and integrated with a Metadata Registry to handle risk concerns in the overall organization environment.**

I. Introduction

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, risk strategies vary from generic approaches, project management, IT (including information security), safety engineering, etc.

Depending on the knowledge area, several definitions of risk can be found in the literature. For instance, in [1] 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 [2] defines risk as: "...the combination of the probability of an event (threat[1]) and its consequences when exploiting any vulnerability[2]".

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 [3]. A RM process describes a set of systematic activities to support the proactive identification and mitigation of risks within a specific environment.

In this paper, we consider that 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 tasks 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 [4], [5]. However, these approaches are not suitable to address the imminent risks that today's organizations face at multiple dimensions (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 II), KAOS [6], GBRM [7] and the Tropos Goal Risk Model [8]. 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 of risk information.

It is currently recognized that RM activities must be aligned with the business processes of the organization [9]. When organization business processes and strategic planning are aligned with proactive RM activities, a well-defined path and

[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 [2].

[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 [2].

978-83-60810-39-2/$25.00

strategy to attain business value is achieved. However, no known business processes have the capability to formally define the sources and dependencies of risks [10]. 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.

In fact, one of the main problems of RM is the fact that several efforts operate in silos with narrowly focused, functionally driven, and disjointed activities [9]. This leads to a fragmented view of risks, each using their own language, customs and metrics. The lack of interconnection and unified 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 formalize the risk management concepts and propose an architecture to manage risk information in an integrated way. This architecture is built on top of three main ideas: (*i*) risks should be mapped into EA artifacts to support an organization-wide view of risks (from the multiple viewpoints defined in the EA), better assess the spread of a risk from a systematic analysis of the EA related components, and improving the monitoring of risks, using the monitoring activities and tracking of changes in the EA; (*ii*) the risks models should be decoupled from the EA representation in order to not depend on a specific representation (e.g., if we propose an extension to a specific notation to include risk information, we would be limited to scenarios where this notation is used); and (*iii*) risk information should be represented in a format that simplifies the interoperability and exchange of information to both internal and external stakeholders or systems.

The remainder of this paper is organized as follows. First, in Section II we describe the related work in the areas of IT Governance, RM and EA. Section III shows the proposed approach to address risks through the EA. Section IV formalizes the risk management concepts, while Section V details the architecture view for the management of risk information. Finally, Section VI presents the main conclusions of this work.

II. Related Work

A. 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.

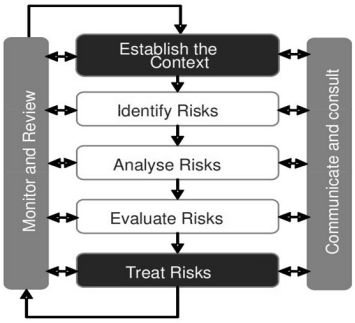

Fig. 1. Risk Management Process

The ISO 31000:2009 RM standard [11] is based on the principle that RM is a process operating at different levels, as shown in Figure 1. 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.

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.

Enterprise Risk Management (ERM) is the process of identifying and analyzing risks, from an integrated and organization-wide perspective [12].

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) view of ERM is that "Every entity exists to provide value for its stakeholders" [13]. 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 [13] 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.

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.

B. IT Governance

IT Governance is a key discipline for making effective decisions and communicating the results within IT-supported organizations. Its main purpose is to identify potential managerial and technical problems before they occur, so that actions can be taken to reduce or eliminate the likelihood and/or impact of these problems. *Control Objectives for Information and related Technology* (COBIT) [14] is a set of best practices, measures and processes to assist the management of IT systems. COBIT is not specific to a technological infrastructure nor business area, and intends to fill the gap between requirements, technical issues and risks. It includes a framework, a set of control goals, audit maps, tools to support its implementation and, especially, a guide for IT management. The latter is organized in the domains of (*i*) Planning and Organization; (*ii*) Acquisitions and Implementation; (*iii*) Delivery and Support; and (*iv*) Monitoring and Evaluation. These processes address the areas of strategic alignment (alignment of IT with the business) [15]; value delivery (creation of business value); resource management (proper management of IT resources); risk management; and performance management.

The "ISO/IEC 27000 series" [16] include a set of standards developed for information security matters. This family of standards specifies the Information Security Management Systems (ISMS) Requirements, proposing a process approach to design, implement, operate, monitor, review, maintain and improve an ISMS. The *design* process follows a risk management approach, including the definition of the risk assessment approach, risk identification, risk analysis, evaluation of risk treatment options and selection of controls to treat risks. The requirements proposed in these standards intend to be generic and applicable to all types of organizations, independent of type, size and nature.

C. 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" [17]. 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

Perspective / Role	DATA What	FUNCTION How	NETWORK Where	PEOPLE Who	TIME When	MOTIVATION Why
Planner (Objective/Scope - Contextual)	Things important for the business	Business Processes	Business Locations	Important Organizations	Events	Business Goals and Strategies
Owner (Enterprise Model – Conceptual)	Conceptual Data / Object Model	Business Process Model	Business Logistics System	Workflow Model	Master Schedule	Business Plan
Designer (System Model –Logical)	Logical Data Model	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Builder (Technology Model – Physical)	Physical Data/Class Model	Technology Design Architecture	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Programmer (Detailed Representation – Out of Context)	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Speculation
User (Functioning Enterprise)	Usable Data	Working Definition	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy

Fig. 2. The Zachman framework

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 [18].

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 [19].

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" [20]. 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 2, 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) [21] 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 that starts with 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).

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.

III. Approach

In other to provide a systematic support to the overall strategy of any organization, being able to map and trace identified risks to enterprise artifacts, this paper proposes an alignment between Risk Management (RM), Governance and Enterprise Architecture (EA) activities. 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 the EA processes. In fact, 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 RM 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 the 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 effectively address the GRC activities of today's organizations [22]. The concepts involved in GRC are not new, but are traditionally addressed as separate concerns inside the organizations. However, these concepts share a set

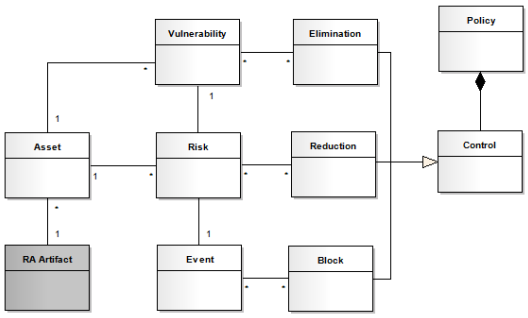

Fig. 3. Domain model of the risk concepts

of knowledge, methodology and processes, which allows an optimal and common 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.

The main rational to propose a connection between Risk and Enterprise Architecture is based on the fact that risk activities are usually performed in silos and without a clear mapping between risks and potentially affected organization components. Extending risk activities to map risks to EA components supports the analysis of 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, which improves the precision and updatability of risk information.

IV. Risk Concepts

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 XML-based Domain Specific Language for RM (Risk-DL), supported by a formal definition of the RM concepts. For mathematical clarity, in this paper we formalize the RM concepts covered in the proposed framework.

To formalize the RM concepts, we use the notation proposed in the relational model [23], where a **relation schema** describes the attributes of each concept, and a **relation instance** is composed by a set of instances of the concepts (tuples) defined in the relation schema. More formally, let $R(f_1 : D_1, ..., f_n : D_n)$ be a relation schema, and for each $f_i, 1 \geq i \leq n$, let Dom_i be the set of values with the domain named Di. An instance of R is a set of tuples, where:

$$\langle f_1 : d_1, ..., f_n : d_n \rangle \, | d_1 \in Dom_1, ..., d_n \in Dom_n$$

Also, we define functions as $f : D- > R$, where f is the name of the function; D is the domain and R is the range of the function. Note that relations can be used to represent the allowed domains or the range of the functions.

Using this notation, the RM concepts are defined in Table I. These concepts are visually modeled by an UML Domain diagram [24] represented in Figure 3.

An **Asset** (A) is any entity which has a value to the organization. Using the proposed language, an asset should be represented by EA artifacts. For instance, an asset can correspond to an entity represented by a cell of the Zachman framework (e.g., business process, program, server). The **Asset Value** is determined by the function A_{Val}. The asset value estimation is decoupled from the asset concept to better integrate distinct types of valuation. We consider three types of valuation: (*i*) quantitative: where the value is estimated by a real number, allowing mathematical calculus to process this values; (*ii*) qualitative: where the value is a qualitative representation, and thus not supporting mathematical calculus; and (*iii*) semi-quantitative: where an initial qualitative value is transformed into a quantitative value to allow mathematical calculus.

Depending on the type of scenario, the asset value function (A_{Val}) can be quantitative, semi-quantitative or qualitative, having D_{Aval} as the admissible range. On the other hand, the value of an asset is not an intrinsic property of the asset "per se", but a result of its integration in a specific environment. Indeed, the same asset can have completely different values if considered in different scenarios (or even if evaluated by stakeholders with different concerns).

A **Vulnerability** (V) identifies a specific characteristic of an asset that exposes its value through a quantifiable **Vulnerability Exposure** (V_E). Again, the fact that the vulnerability exposure can be determined by quantitative, semi-quantitative and qualitative methods, explains the decoupling of this function from the concept of vulnerability.

An **Event** (E) represents any uncontrolled circumstance that has the ability to produce consequences on the value of assets. Again, the event is quantified by an **Event Likelihood** (E_L) that can be determined by quantitative, semi-quantitative or qualitative methods. Considering quantitative values, the likelihood of the event cannot be 0% neither 100%. In fact, events that will never occour do not introduce any type of risks, while events that are certain to occur are known facts (if we know that an important technician will retire next month, we can not say that we have a risk of loosing that technician, since it is a fact).

A **Risk** (R) is determined by a triple composed by the event that can exploit a vulnerability of a specific asset. The **Risk Severity** is modeled by a function (R_S) to quantify the impact that occurs if the event is able to exploit the vulnerability of the asset defined in this risk. Once again, this function can produce quantitative, semi-quantitative and qualitative results.

A **Control** (C) is used to manage risks, trying to mitigate them. We propose three types of controls. First, a **Block Control** (C_B) is a control to limit the probability of an event to occur. This way, a block control represents a function that determines a new likelihood for an event. This function has the same range (D_{EL}) of the event likelihood function. Second, an **Elimination Control** (C_E) intends to reduce the exposure of a vulnerability. This way, it determines a new exposure, using the same range (D_{VE}) of the vulnerability exposure function. Finally, the **Reduction Control** (C_R) assumes that the risk occurs and pretends to reduce its consequences, producing a result on

TABLE I
FORMALIZATION OF RISK MANAGEMENT CONCEPTS

Concept	Formalization	Description
Asset	$A(aName : string, aType : D_{atype}, aRef : D_{aRef}, a_1 : D_1, ..., a_n : D_n)$	D_{atype} determines the domain of asset types; D_{aRef} determines the reference of the asset to the EA.
Asset Value	$A_{Val} : A- > D_{Aval}$	Asset value (quantitative, semi-quantitative or qualitative).
Vulnerability	$V(name : string, vType : D_{vType}, asset : A)$	Identifies a vulnerability in an asset defined in A. An asset can have several vulnerabilities.
Vulnerability Exposure	$V_E : V- > D_{VE}$	Function that determines the exposure of the vulnerability.
Event	$E(name : string, eType : D_{eType})$	it can be a threat (bad event) or an opportunity (positive event).
Event Likelihood	$E_L : E- > D_{EL}$	Initial estimation of the probability of occurrence of an event.
Risk	$R(E, A, V)$	Consequences that an event produce when exploiting a vulnerability.
Risk Severity	$R_S : R- > D_{RS}$	Severity of the impact produced by the occurrence of the risk.
Block Control	$C_B : E- > D_{EL}$	Control to block the event (reducing its probability).
Elimination Control	$C_E : V- > D_{VE}$	Control to eliminate a vulnerability (reducing its exposure).
Reduction Control	$C_R : R- > D_{RS}$	Control to reduce the severity of the impact produced by a risk.
Control	$C \equiv C_B \cup C_E \cup C_R$	Actions that can be taken to mitigate risks.
Cost	$Cost : C- > D_C$	Cost of implementing a control.
Policy	$P \equiv C_1, C_2, ..., C_n$	where $C_i \in C$

the range (D_{RS}) has happens in the risk severity function.

The adoption of a specific control has a **Cost** (*Cost*) to the organization, which can also be determined in a quantitative, semi-quantitative or qualitative way.

Finally, the concept of **Policy** (*P*) defines the set of controls that are managing the risks identified in a specific organization. Ideally, organizations procure an optimal policy to effectively handle risks at a minimum cost.

Note that the ranges: $D_{atype}, D_{aRef}, D_{Aval}, D_{vType}, D_{eType}, D_{EL}, D_{VE}, D_{RS}, D_C$ have to be defined (in qualitative assessment, these ranges define the risk matrices). For instance, D_{Aval} can be defined as: $D_{Aval} \equiv \{low, medium, high\}$, meaning that the asset values can be qualitatively quantified by low, medium or high.

V. MANAGING RISKS USING RISK-DL

Risk-DL is a XML[3] based vocabulary and schema to represent the risk concepts defined in Section IV. In fact, the Risk-DL defines the XML Schema[4], in the form of a *.xsd* file, that should be used to create XML files defining risks.

The main objectives of Risk-DL include, but are not limited to: support interoperability between distinct sources of risk information; support of sharing, discovery, reuse and processing of risk information; enable the alignment between risks and organization artifacts, by linking assets to records (e.g., business processes) managed within an organization EA; reduce inconsistencies by formalizing the risk concepts; provide an open specification that enables risk information to be categorized and support human-machine and machine-machine interoperability, either internally when different units produce risk information or externally across multiple organizations. Also, XML uses a human language that can be easily understood by people and computers, being highly portable and platform independent. Moreover, this solution also takes advantage of common XML properties, like its extensibility, which simplifies the evolution of Rik-DL, as well as the assurance of compatibility between different versions of the same language.

Figure 4 shows an excerpt of the Risk-DL definition *.xsd* file (left side) and an example of *XML* file defining an asset. In this example, the *BP1.2.3 Central data validation* is a business process defined in the EA. Both the asset type and value are previously defined in the *XML* file (omitted in the paper due to space limitations).

The use of a formalized *XML* representation for risk information, facilitates the automatic definition of risk information. For instance, an organization that has an *Asset Management* system, or a *Configuration Management Database*, can define mappings to automatically generate the Risk-DL structure to represent assets. This fact, not only simplifies the Risk Management process, but also increases the quality and alignment between risk activities and other organization processes.

The proposed overall solution to manage risk information is detailed in Figure 5. An 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 Metadata Registry (MDR) component. The use of a MDR intends to ensure interoperability between different risk representations, as proposed by ISO/IEC 11179 [25], 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

[3]http://www.w3.org/XML
[4]http://www.w3.org/XML/Schema

```
<xs:element name="asset">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="riskdl:name"/>
      <xs:element ref="riskdl:asset-Type"/>
      <xs:element ref="riskdl:description"/>
      <xs:element ref="riskdl:asset-value"/>
      <xs:element ref="riskdl:properties"/>
      <xs:element ref="riskdl:vulnerabilities"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="asset-Type" type="xs:NCName"/>
<xs:element name="asset-value" type="xs:NCName"/>
<xs:element name="properties">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="riskdl:property"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="property">
  <xs:complexType>
    <xs:attribute name="name" use="required"/>
    <xs:attribute name="value" use="required"/>
  </xs:complexType>
</xs:element>
```

```
<asset>
    <name>BP1.2.3 Central data validation</name>
    <asset-Type>Process</asset-Type>
    <description>GestBarragens Central data validation</description>
    <asset-value>medium</asset-value>
    <properties>
        <property name="BP name" value="Data valiadation"></property>
        <property name="Inputs" value="BP1, BP2"></property>
        <property name="Specification" value="bpel"></property>
        <property name="File" value="centralDataVal.bpel"></property>
    </properties>
    <vulnerabilities>
        <vulnerability>
            <name>Lack of metadata</name>
            <vulnerability-Type>Process</vulnerability-Type>
            <vulnerability-Exposure>medium-high</vulnerability-Exposure>
        </vulnerability>
        <vulnerability>
            <name>Lack of qualified staff</name>
            <vulnerability-Type>Process</vulnerability-Type>
            <vulnerability-Exposure>very-high</vulnerability-Exposure>
        </vulnerability>
    </vulnerabilities>
</asset>
```

Fig. 4. Risk-DL example

objects. This way, the syntactic representation of the Risk-DL language is irrelevant for the overall purpose of this solution.

Consequently, the architecture supports different versions of Risk-DL, as well as other risk representations. The Operator can manually define the risk information (using a web interface) or automatically transform its specific format to represent risk information (e.g., the asset list) into Risk-DL. Automatic transformations are supported by the MDR component if specific risk format is registered into the MDR. The mapping between a specific format and Risk-DL are partially inferred by the MDR (if the mapping is not complete, the MDR component provides an interface to specify schema mappings). 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 (XML file) and generates an internal Risk Representation (a set of *Java* objects) 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 Plan Generator proposes controls based on the Risk Library, but other controls can be specified through Risk-DL. Based on the available controls, the set of Risk Plans is generated.

The Risk Library represents a risk knowledge base, locally storing validated risk information as, for 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 III. 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 the organization), supporting a common 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

VI. Conclusion

Risks exist everywhere and everyday, whether or not it is recognized by the stakeholders affected by them. One of the main challenges that the risk community has to address is on the modeling of risk information. In fact, among other issues, risks involve a highly heterogeneous set of assets, events, methods, stakeholders and responsibilities, requiring adaptable methods and tools to support the exchange and interoperability of risk information. On the other hand, RM in general and risk assessment in particular, tend to be done in silos, by distinct teams with potential different views on the same risks.

This type of issues are commonly addressed by the EA community, where organizations are modeled from multiple views and different concerns of the involved stakeholders (viewpoints). In this paper, we propose to take advantage of the EA methods and best practices to facilitate the exchange

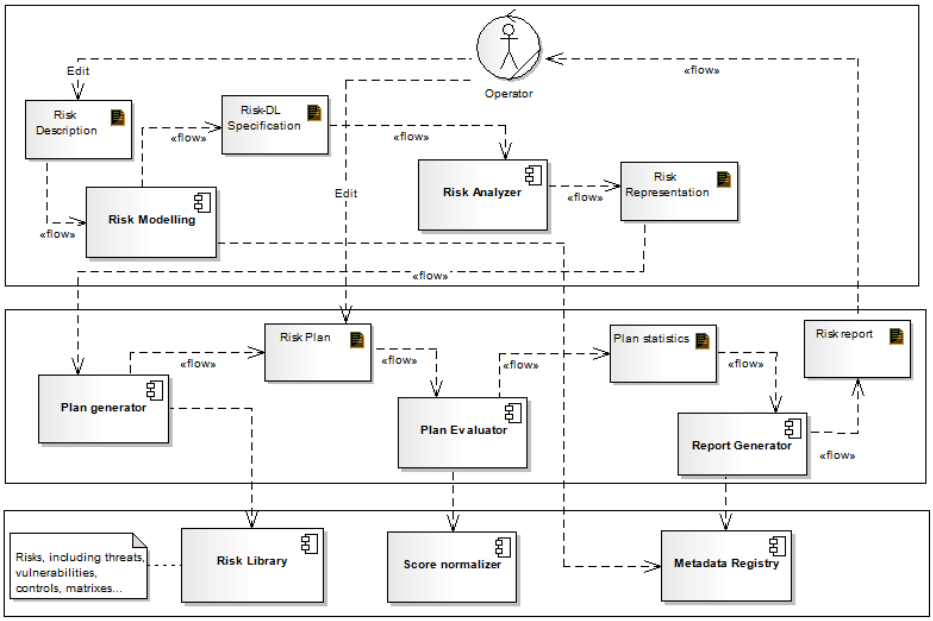

Fig. 5. Solution Overview

of risk information, as well as providing an organization-wide view on risks. As a consequence, risks can be tracked back to EA artifacts, allowing a detailed and precise analysis of the spreading of a specific risk.

We propose a solution that is decoupled from any risk or EA representation, so that it does not depend on any formalism. The proposed solution includes a XML-based language to formalize risks and integrate a Metadata Registry to support the communication with different risk representations, as well as providing different views to communicate risk information to the stakeholders.

ACKNOWLEDGMENT

This work was supported by FCT (INESC-ID multi-annual 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] I. Sommerville, *Software Engineering (7th Edition)*. Addison Wesley, 2004.
[2] "ISO Guide 73:2009. Risk management – Vocabulary," 2009.
[3] "Software Engineering Institute. Capability Mautiry Model Integration for Development. Version 1.3," Carnegie Mellon University, November 2010.
[4] M. Stamatelatos, W. Vesely, J. Dugan, J. Fragola, J. Minarick, and J. Railsback, "Fault tree handbook with aerospace applications," NASA, 2002.
[5] *DoD: Military Standard, Procedures for Performing a Failure Mode, Effects, and Critical Analysis (MIL-STD-1692A). US Department of Defense*, 1980.
[6] A. Dardenne, A. van Lamsweerde, and S. Fickas, "Goal-directed requirements acquisition," in *Science of Computer Programming*, vol. 20, 1993, pp. 3–50.
[7] A. Anton, "Goal-based requirements analysis," in *International Conference on Requirements Engineering*, IEEE Computer Society. Washington DDC, USA: IEEE Computer Society, 1996.
[8] Y. Asnar and P. Giorgini, "Modelling risk and identiffying contermeasure in organizations," in *CRITIS*, J. Lopez, Ed. Springer-Verlag, 2006, pp. 55 – 66.
[9] S. Maziol, "Risk management: Protect and maximize stakeholder value," Oracle Governance, Risk, and Compliance, White Paper, February 2009.
[10] S. Biazzo, "Process mapping techniques and organisational analysis: Lessons from sociotechnical system theory," *Business Process Management Journal*, vol. 8, no. 1, pp. 42–52, 2002.
[11] "ISO 31000:2009. Risk management – Principles and guidelines," 2009.
[12] "Managing Risk from the Mailroom to the Boardroom," June 2003.
[13] "Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management - Integrated Framework," 2004.
[14] "IT Governance Institute. CobiT 4.1. Framework – Control Objectives – Management Guidelinces – Maturity Models," 2007.
[15] W. V. Grembergen, *Strategies for information technology governance*. Idea Group Publishing, 2003.
[16] "ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements," 2005.
[17] "IEEE 1471:2000 - Recommended Practice for Architectural Description for Software-Intensive Systems," 2001.
[18] T. Mens, J. Magee, and B. Rumpe, "Evolving software architecture descriptions of critical systems," *Computer*, vol. 43, pp. 42–48, 2010.
[19] P. Sousa, A. Caetano, V. A., C. Pereira, and J. Tribolet, "Enterprise architecture modeling with the unified modeling language," in *IGI Global*, 2006.
[20] J. Zachman, "A framework for information systems architecture," *IBM Systems Journal*, vol. 12, no. 6, pp. 276–292, 1987.
[21] "The Open Group. TOGAF Version 9. Zaltbommel, Netherlands: Van Haren Publishing," 2009.
[22] M. Frigo and R. Anderson, "A strategic framework for governance, risk, and compliance," *Strategic Finance*, vol. 90, no. 8, February 2009.
[23] R. Ramakrishnan and J. Gehrke, *Database Management Systems (Second Edition)*. McGRAW-HILL International Editions, 2000.
[24] "ISO/IEC 19501:2005. Unified modeling language specification, v. 1.4.2 formal/05-04-01," January 2005.
[25] "ISO/IEC 11179-1:2004. Information Technology – Metadata Registries (MDR) – Part 1: Framework," 2004.