Multi-Viewpoints Ontology of Risk Management

Ricardo Vieira¹ ² José Borbinha¹ [supervisor]

¹ Instituto Superior Técnico, Universidade Lisboa, Lisboa, Portugal
² INESC-ID, Lisboa, Portugal
{rjcv,jlb}@tecnico.ulisboa.pt

Abstract. Risk management is the process of managing uncertainty through the identification, analysis, evaluation and treatment of risks. In a real scenario, the process must be closely aligned with the business, meaning the concepts, techniques and practices suitable for risk management application have a strong dependency from the context of the problem. In a first moment that lead to a proliferation of specialized frameworks defining how risk management should be established and implemented in specific domains, and therefore privileging specific viewpoints. However, if on one side that can prove to be effective, the specialization can also be a limitation to the practice of risk management in scenarios of multiple heterogeneous domains, which is increasingly a common need in the enterprise world. Consequently, there is a need to solve the problem of integrating or simply reconciling several domains in common contexts, a challenge recognized in the literature. This work intends to address that problem, proposing to contribute for its solution by suggesting that an adequate conceptualization using a multi-viewpoints ontology alignment at a meta-model level can support the definition, integration and reconciliation of risk management multiple viewpoints.

Keywords: Risk Management, Enterprise Risk Management, Ontology Engineering.

1 Problem Description and Motivation

Governance, Risk and Compliance (GRC) are three essential pillars in any organization, which always must be addressed as a whole. Governance ensures that the organization is capable of achieving its objectives. Risk ensures that the uncertainty on the achievement of objectives are managed. Compliance ensures the organization adheres to existing policies, procedures, laws and regulations. Risk Management (RM) is the pillar that must influence the awareness of Governance concerning the risks that may affect the achievement of the objectives, and of Compliance concerning how the business processes realize requirements of the context.

The complexity of RM and its increasing importance has led to a proliferation of frameworks that define how RM should be established and implemented. Due to the diversity of business where RM can be applied, RM frameworks typically focus on specific domains. For instance, Information Security is a domain where RM is well recognized due to existence of known references such as, among others, ISSDRM [1].
OCTAVE [2], and most recently ISO27005 [3]. In the domain of Information Technology Governance, RM is usually defined through references such as Control Objectives for Information and related Technology (COBIT) [4] and Risk IT [5]. The diversity of contexts where RM can be applied, together with the proliferation of domain-specific knowledge, created several fragmented viewpoints, with different languages, parameterizations, and metrics [6]. Consequently, and due to the lack of uniformity regarding the development of RM systems and tools, it is usual to see organizations using specific-built solutions that cannot be reused in other contexts or organizations [6]. This created a problem, especially at the strategic management of organizations, which often imply to analyse risk reports with different processes and concepts from several departments (e.g. financial department vs the IT Governance department). In other words, because of the efforts of defining RM in different domains, RM tends to operate in silos with narrowly focused, functionally driven, and disjointed RM activities, which can be a problem for corporate risk management.

2 Risk Management

Risk management can be defined as the “coordinated activities to direct and control an organization with regard to risk – the effect of uncertainty on objectives” [7]. RM must be therefore understood as a process to coordinate the set of activities required to manage policies, procedures and practices in RM. A typical RM process, according to ISO 31000 [7], is an iterative process where, as the first step, the context should be established in order to identify internal and external factors that can influence the remaining activities of the process. Risk assessment is the sub-process of identifying existing risks in the pre-defined context, analyzing the identified risks typically regarding its severity, and evaluation where identified risks are compared using the previous analysis in order to prioritize treatment. Using the output of risk assessment, in risk treatment, stakeholders define a risk treatment plan that consists of a set of controls (actions) that mitigate the identified risks. Throughout the mentioned activities is essential that all relevant stakeholders are consulted and informed (communication and consultation phase) to assure accurate identifications and estimations. Additionally, the risk information defined in each activity should be constantly monitored (monitoring and review phase) in order to assure that it is constantly updated.

2.1 Risk Management in Context

RM can be applied in several contexts and for different purposes. Therefore, a crucial aspect of any RM process is to establish its context, which comprises mainly setting the scope and objectives [7]. In general, RM deals with the uncertainty that is present in any business or activity, but its drivers and benefits can greatly vary [7]. One of the most common misconceptions regarding RM is that it merely focusses on preventing unexpected losses [8]. However, when properly defined, risk is “a deviation from the expected – positive or negative.” [7]. Therefore, a risk can represent a threat to the achievement of an objective, but also an opportunity to be explored [7]. The recognition
of the benefits and outcomes of RM has led several domains of expertise to recognize it as an essential activity:

- **COBIT** [4] defines best practices and processes for **IT Governance**. Each COBIT process is linked to a set of goals, resources and activities. Within those processes, it is possible to identify several RM activities considered essential to the Governance of IT. Additionally, one of the reference processes is precisely “Manage Risk”, which has the goal of aligning the objectives of IT management with Enterprise RM (ERM), thus using RM has a driver for balancing costs and benefit when managing IT-related enterprise risks [4]. The risk processes and activities presented in the present version of COBIT, COBIT5, are inspired from Risk IT [5].

- **Project Management** is the process of managing activities and resources to achieve established goals and objectives. The Project Management Body of Knowledge (PMBOK) [9], developed by the Project Management Institute (PMI), defines best practices with regard to project management. The PMBOK is organized into nine knowledge areas, decomposed into processes groups and processes. One of the knowledge areas is RM, which deals with identifying, analysing and responding to project risk to minimize uncertainty regarding the achievement of the project goals [9]. PRINCE2 [10], from “Projects IN Controlled Environments, version 2”, is a process-based method for effective project management that is used extensively as a best practice method. PRINCE2 defines a set of “processes, principles and themes” essential for project management. One of the aspects addressed is risk, being recommended that any project should maintain a log of risks that may threaten the achievement of the project goals [10] (a concept also known as “risk register”).

- **Process Improvement** refers to the organizational practice of assessing and improving existing business processes in order to achieve a better quality of service [11]. The Capability Maturity Model Integration (CMMI) [11] was developed by the Software Engineering Institute of the Carnegie Mellon University, and aims to establish best practices and methods for the design and creation of maturity models for processes. A maturity model consists of a number of ‘maturity levels’ that describe increasing levels of process quality (or levels maturity) [11]. CMMI defines that maturity models can have two types of representations: continuous and staged. The former, structures processes and processes areas into maturity levels so that an organization can understand which requirements are necessary to comply each level of maturity. The staged representation decomposes processes areas into goals, i.e. for each process area level, a set of goals to be achieved is defined. Anyway, the process areas defined for both representations are (1) Process Management, (2) Project Management, (3) Engineering, and (4) Support. One of the requirements or goals for the Project Management process area is precisely RM with the goals of (1) establish the context for RM, (2) perform risk assessment and (3) mitigate risks [11].

- **Information Security** refers to the processes and methods intended to protect information asset from existing threats, such as unauthorized access, modification, destruction, etc. Therefore, one of the essential aspects of information security is to assess information security risks and mitigate them [12]. The ISO/IEC 27000 Series
of Standards [12] and the Factor Analysis of Information Risk (FAIR) [13] [14] are among the most known references in this domain.

- **Financial risk** is the risk associated with financial transactions. The Basel Accords are recommendations on banking regulations issued by the Basel Committee on Banking Supervision. Basel I [15], the first issued Accord published in 1988, defined financial risks as credit risks and market risks. The former is the risk of a borrower not paying a specific debt. The latter refers to the risk related to market fluctuations. As defined in the regulation the main objective of financial risk. Traditionally, RM in this domain focus on the risk factors that might trigger credit or market risks. However, Basel II [16] , published in 2004, recognized that banking institutions should also manage operational risks, i.e. risks not specific to the financial domain that occur in a normal course of any business activity such as risks related to legal aspects, reputation, process management, etc [15].

Note that different contexts might lead to different focus on RM. For example, in financial RM, it is common to assume that all financial institutions are subject to a common general context, therefore to the same classes of risks: credit risk, market risk, interest rate risk, etc. This implies that a common context is stablished and shared conceptual reference models are already well stablished, and thus the main focus of RM is usually on specializing these models for the local deployments. The same occurs, for example, in the domains of insurance, infrastructure and healthcare. Consequently, research in those domains focuses mainly on the identification of individual risks sources, and in the definition of the corresponding analytical and statistical models that allow estimating how these individual risks sources influence the estimated likelihood and consequence of the (pre-defined) risks. In other words, we can say that in domains already well stablished, where common regulations or high level of maturity and common conceptual models already exist, leaving the focus of RM to merely one activity, risk analysis. The main motivation for this work is not to specialize even more any of those domains, but to contribute for the problem of how integrate multiple domains, a problem requiring addressing all activities of a complete RM process.

### 2.2 Enterprise Risk Management

As described before, the diversity of RM domain-specific contexts promoted fragmented visions of RM with their own specific concepts. Consequently, RM tends to operate in silos that prevent the collaboration between risk experts within a same organization. This can lead to duplication of RM efforts and production of risk information impossible to aggregate and reuse at an organizational level.

Enterprise Risk Management (ERM) is the process of managing risk across an organization recognizing the existing of different levels and units of operation within RM [17]. ERM intends to assure that (1) risks are assessed and treated trough the organization; (2) there is a common understanding of RM through the organization; (3) stakeholders are aware of the organization risks and their responsibilities in the RM process; (4) governance and risk are inextricably linked; and (5) the organization is able to respond to a changing business environment.
ISO31000:2009 [7] greatly contributed to the harmonization of existing domains and the development of ERM Frameworks by defining general principles and a process for RM independently of its domain of application. Additionally, COSO ERM provided one of the most known frameworks for ERM that consequently motivated the proliferation of ERM Frameworks.

The common strategy of ERM is to provide a common process, terminology and techniques to use across the organization. The approach, while valid, hinders the use of domain-specific RM processes, terminologies, and techniques that can potentially be more effective and efficient. Additionally, for the organizations that followed the traditional and disjointed RM processes and intend to improve to an ERM centric RM process, this typically implies the loss of already existing risk information or, if possible, adapting the existing information.

3 Ontology Engineering

Ontology Engineering is a discipline that studies the methods for building an ontology. “An ontology is a formal, explicit specification of a shared conceptualization” [18]. A “conceptualization” refers to an abstract subjective view that we may have in our minds regarding a concrete aspect of the world [19]. Therefore, an ontology intends to represent a conceptualization using an explicit formal specification, in a machine-readable language that intentional constrains the interpretation of the conceptualization through a set of suitable axioms [19]. Finally, “a shared conceptualization” means that the ontology stakeholders must agree on the definitions of the axioms primitives, and that the ontology “captures consensual knowledge” shared among the stakeholders [18].

An ontology can be classified according to its scope and objective (as shown in Fig. 1):

- An upper ontology (also known as top-level ontology) describes general and abstract concepts pertaining to the universe such as space, time, object, action, etc. [20]. An ontology of that kind is independent of a particular problem or domain. Its objective is to improve the “shared” characteristic of the “consensual knowledge” by providing detailed definition of primitive abstract concepts.
- A domain ontology describes concepts pertaining to a particular domain (e.g. medicine, computer science, etc.) [20]. The objective of such ontology is to promote the reuse of common concepts across the domain. A domain ontology can be defined by specializing concepts of a top-level ontology.
- A task ontology describes concepts pertaining to one or more tasks [20]. Typically, the defined tasks are used to solve a problem within a particular domain. The objective is to promote common solutions to typical problems.
- An application ontology describes a domain-specific application and depend on both a domain and a task ontology [20]. An application ontology might contain concepts pertaining to a particular application in the domain but that are not shared across the overall domain.
Note that there is a distinction between ontologies and a knowledge base. An ontology defines concepts, relationships, and axioms assumed to always be true by the ontology stakeholders [20]. A knowledge base might describe facts and assertions only valid to “a particular state of affairs or a particular epistemic state” [20]. Nevertheless, a knowledge base should be aligned with a particular ontology. In fact, the creation of a knowledge base consists of populating an ontology with a particular set of objects. Therefore, a knowledge base is an instantiation of an ontology.

3.1 Description Logics

As stated before, an ontology represents shared knowledge using machine-readable languages. Description Logics (DL) are a family of knowledge representation languages commonly used to represent knowledge. DL are logic languages in the sense that there are built from atomic concepts and roles that allow the representation of logic-based semantics [19]. Additionally, DL typically allow assertion formalism that allows, for example, the declaration of complex axioms using simpler pre-defined axioms. In other words, it allows the definition of concepts using composition and specialization. This essential characteristic supports “inference capabilities that deduce implicit knowledge from explicitly represented knowledge” [19].

The suitability of DL as ontology languages has known its peak with the introduction of several web ontology languages, in particular OWL, an ontology language standard developed by the W3C Web-Ontology Working Group¹. OWL is based on a RDF schema, where an atomic concept corresponds to class, an atomic role corresponds to a property and a concrete object (an instantiation of a concept) corresponds to an object. A representation of an ontology in OWL consists in a set of axioms that constrain the

¹ http://www.w3.org/2001/sw/WebOnt/
mentioned OWL primitives. As any DL, the definition of classes in OWL can use composition or specialization. Additionally, OWL properties can be restricted using predefined functions that add specific characteristics to the property. For example, OWL allows the definition of symmetric properties between OWL objects, meaning that a particular property that relates object A to B can be inferred to also relate B to A through the same property.

3.2 Ontology Engineering Methods

An ontology development method consists on a set of activities to develop an ontology. This section presents a brief discussion on the state of the art of ontology engineering development methods.

Ushold and King [21] developed one of the first methods when researching on how to build an Enterprise Ontology. The process consists on, first, identify and define the ontology purpose, then build the ontology through the identification and representation of conceptualizations. Additionally, if required, the ontology should consider any other upper or domain ontology that relate with the concepts being defined. Finally, the ontology should be properly evaluated and documented according to the guidelines defined in the method.

Similarly, Gruninger and Fox [22] developed a method for the enterprise domain. This method defines that the development process should start with the identification of requirements (purpose and scope of the ontology) using informal descriptions along with motivation scenarios for the ontology. The scenarios should then evolve to a set of competency questions defined in formal language. Competency questions define the set of problems that the ontology intends to solve and restrict the possible solutions by indicating what should be expected as answer to the questions. Each competency question should be answered through a set of first-order logic axioms. Finally, competency questions should be related through completeness theorems that describe how the questions relate between them in the domain of discourse.

The project KACTUS [23] proposes a method to build an ontology using a bottom-up approach. Ontology stakeholders should start by defining the application ontology related to the specific domain and only later generalize the conceptualizations to a domain ontology. The argument is that if the process is iteratively and constantly executed the resulting domain ontology always represent the shared knowledge of the stakeholders.

METHONTOLOGY [24][25] is a method introduced to provide detailed descriptions of the already identify activities of an ontology building process. METHONTOLOGY includes an ontology development process, an ontology life cycle and a method itself. Regarding the process activities, METHONTOLOGY aligns, in general, with other processes and establishes that developing an ontology consists of specification, knowledge acquisition, conceptualization, integration, implementation, evaluation and documentation. The METHONTOLOGY life cycle motivates the definition of support activities for the different stages an ontology goes through its lifetime such as control, evolution and quality control. Finally, the method goes in detail about
the mention activities: the steps to cover, the techniques to use and their input/output; and how to evaluate and document activities.

3.3 Ontology Engineering in Risk Management

The application of ontology engineering in RM applications can be found in the literature. In [26], the authors developed a task ontology for the application of the risk assessment technique entitled FMEA for the pharmaceutic domain. AURUM [27] is a method for supporting the NIST SP 800-30 [28] RM standard, that provides an information security ontology where the concept of risk is defined. Similarly, the Risk-Oriented Process Evaluation (ROPE) [29] includes a security ontology to support a RM process in information security. In [30] an ontology of typical software management risks is presented in order to support risk identification in software project management. Henk Birkholz et. Al.[31] introduced the idea that by modelling the assets of organization, their dependencies and relationships in an ontology, it is possible to define a reasoning process that automatically identifies risk. The MONITOR risk ontology [32] describes RM in the context of disaster management. OntoBacen [33] represents the conceptualization and definition of business rules present in governance policies of the Brazilian financial system, where it is possible to identify the representation of what constitutes financial risk.

Similar to the work here being proposed, Giancarlo and Rossella [34] recognize that RM can be applied in several different domains. That diversity itself constitutes a risk if different contexts use different conceptualizations of the core RM concepts. Therefore, the authors introduce a RM ontology to serve as a meta-model for several RM applications. This ontology uses an analogy where it is argued that the RM systems are equivalent to sensor networking systems. Therefore, the ontology is developed using a rule-based logic language called RSF [35], a sensor network language that allow defining reactive systems in terms of event-condition-transition rules. To validate the approach, the ontology is used in two RM case studies in the domain of distributed software projects and environmental management respectively. The purpose of the solution is similar to ERM: a common framework is defined to implement RM in different contexts. As a relevant solution to ERM, the approach is valid, but it still hinders the value of domain-specific RM processes, concepts, and techniques that can potentially be more effective or efficient.

4 Research Statement

The diversity of RM domain-specific contexts promoted fragmented visions. Consequently, RM tends to operate in silos that prevent the collaboration between risk experts within a same organization. This can lead to duplication of efforts and production of risk information impossible to aggregate and reuse at an organizational level. ERM is the practice of managing risks in an organization. ERM usual strategy to solve the problem of isolation is to promote a common framework, with process, concepts and practices imposed across the organization. This approach, while valid, hinders the value
of RM processes, concepts, and techniques that can potentially be more effective or efficient for each specific domain. Additionally, in scenarios where organizations already possess heterogeneous risk information produced through the implementation of specialized RM processes, the migration process to an ERM approach can be difficult, leading to potential loss of existing risk information (as also to the loss of effectiveness). Finally, specialized RM can be unavoidable in scenarios where external factors might impose specific RM frameworks for specific domains (such as for compliance).

Therefore, it is desirable to have solutions that enable the use of domain-specific practices that, at the same time, enable the communication and reuse of risk information from domain-specific contexts. As a result, this work grounds in the following research question:

**Research Question.** How to implement risk management in contexts with multiple stakeholders and concerns without restricting the use of domain-specific processes, terminologies, and techniques?

In conceptual modelling, the concepts of viewpoint and view comprehend and manage complex domains where multiple stakeholders with different concerns exist. A view must express the perspective of specific concerns of a set of stakeholders. A viewpoint “establishes the conventions for the construction, interpretation and use” of a view [36]. As stated in ERM frameworks, stakeholders are aware of other concerns so it is not a problem of awareness but rather of not possessing the capability to define their own RM view without impeding the relation with other RM views.

A RM viewpoint within a specific context must comprise the definition of the concepts, and relationships among them, to use in the RM process to express risk in that context. For example, one RM viewpoint can define risk by the concepts of event and consequence, while other viewpoint can define it by the concepts of threat and vulnerability. In addition, different viewpoints might require different risk assessment and communication techniques. For example, a typical RM matrix can only be effective if it is possible to estimate risk probability and impact; also, a bow-tie diagram is typically a technique suitable for contexts where the concepts of threat, hazard and consequence exist. In conclusion, the definition of a RM viewpoint must be an essential concern since it influences the output of the RM process; failing doing that might result in the impossibility of using the intended assessment and reporting techniques. Therefore, it is important to address those concerns early, during the establishing of the context activity, and considering the objectives for the RM process.

A domain ontology explicitly describes the knowledge implicitly shared by a set of stakeholders in a particular domain. In complex domains with multiple viewpoints the same aspects of the domain can use different representations depending of the context of application. Recently, there has been increasing research on viewpoints-based approach for problems of multiple ontological representations [37][38][39]. There are two classes of ontology-based integration approaches: “a priori” or “a posteriori” [40]. In the former, the definition of each ontology uses a global ontology that relates all concepts. In the latter, the definition of each ontology is independent, and the definition of correspondence rules is necessary to allow their integration. Multi-viewpoint integration uses both approaches. Through the use of primitives such as global concept, local
concept, local role, local interpretation, among others, a multi-viewpoint domain ontology enables the definition of multiple representations [39]. Therefore, a domain ontology still represents the core aspects of the domain, but at the same time, the specialization of the domain is possible through the integration of multiple viewpoints developed independently. In short, multi-viewpoints ontology integration define the domain at a meta-model level in order to support the definition of different possible conceptualizations, according to different stakeholder’s perspectives [41]. As such, we formulate the following hypotheses statements for addressing the research questions (ordered from the most specific to the most generic):

| Hypothesis 1 (H1) | The body of knowledge of ontology technology can provide an effective support to knowledge management in Enterprise Risk Management. |
| Hypothesis 2 (H2) | It is possible to express guidelines for the effective definition of Risk Management specific viewpoints using the current ontology engineering state of the art. |
| Hypothesis 3 (H3) | An adequate conceptualization using multi-viewpoints ontology alignment at a meta-model level can support the definition, integration and reconciliation of Risk Management multiple viewpoints. |

In order to address the defined hypothesis the solution artefact should be composed following elements (see Fig. 2):

- **Domain ontology.** In order to demonstrate H3, a risk management domain ontology should be developed. The ontology should represent the core knowledge shared between the risk management viewpoints. The ontology should be developed according to principles of multi-viewpoint ontology alignment to ensure that it can be specialized to represent the risk management viewpoints.

- **Application ontology.** In order to demonstrate H2, an application domain ontology should be developed for each of the risk management viewpoints. Any application ontology should be a specialization of the domain ontology. The development of any application ontology should be based on a pre-defined set of principles and guidelines.

- **Task ontology.** A challenge in ERM is how to use heterogeneous risk information from multiple data sources. The challenge results from the diversity of domain-specific contexts but also from the diversity of RM techniques. For example, ISO 31010 [42] describes 31 techniques to perform risk assessment depending on the resources and skills of the context of application. Therefore, in order to support ERM (and consequently demonstrate H1) a task ontology should be developed for each RM technique.

- **Knowledge base.** In order to validate the solution artefact it is necessary to demonstrate its possible uses to meet real needs. Therefore, it is necessary to instantiate a set of application ontologies and consequently develop multiple knowledge bases. The solution artefact should enable the aggregation and reuse of risk knowledge between different knowledge bases consequently validating all hypothesis.
For final consideration note that the proposed architecture aligns with the M3-Model of the Meta-Object Facility (MOF) [43] where each element on every layer is an instantiation of the layer above. The metamodeling architecture of MOF defines the Unified Modeling Language (UML). In fact, the proposed solution could, in principle, be conceived in UML. The rationale for OWL was that the proposed solution will enable reasoning capabilities that potentially can be useful for certain RM activities such as risk analysis and evaluation. However, that is currently out of the scope of this work.

5 Work Plan

The research method taken in this work is based on the design science research method (DSRM) as described in [44]. DSRM is comprised by the following activities:

- **Awareness of problem.** The researcher brings awareness of a specific problem in an industry or discipline. The research proposes to formal or informal pursue answers for the identified problem.
- **Suggestion.** The research studies the existing body of knowledge/theory for the problem area in order to envision a possible solution. Suggestion is a creative step where the researchers innovatively combines new or existing elements to imagine a solution. The step should result in a tentative design of the solution, i.e. an abstract definition of how the solution will be constructed and what potential benefits it might bring to the problem area.
- **Development.** The tentative design defined in the previous step is developed at this phase. The development method can vary depending of the expected artefact type.
- **Evaluation.** Once constructed, the artefact must be evaluated to ensure that all intended goals were achieved. The goals for the artefact should been defined in the
proposal at the awareness of problem step. Evaluation should clearly define the process of evaluation and the implicit criteria that should be met through evaluation.

- **Conclusion.** The conclusion ends the research by judging the achieved results: how well the solution addresses the identified problem, its potential and limitation. Conclusion marks the stage when the researcher is able to finalize the research by providing evidence (typically in form of a written report) of its research process and achieved results.

Suggestion, Development, and Evaluation are typically iteratively performed through the research process. The steps represent the circumscription process that has the goal of generating “understanding that could only be gained from the specific act of construction” [44].

The work proposal here described in this document represent the proposal and tentative design of this research project – the outputs of the awareness of problem and suggestion process steps. Regarding the development phase, the research project has defined three hypothesis that should be demonstrated by the solution artefact components detailed in section 4. For the evaluation activities, we propose two types of evaluation:

- **Theoretical Evaluation.** This evaluation will use the body of knowledge of RM to demonstrate, in theory, the correctness of the domain ontology. Particularly, the ontology should demonstrate that it can be instantiated into an application ontology that accurately represents the RM viewpoints defined in the existing RM frameworks. Similarly, and using public and available RM knowledge (e.g. from real cases reported in conferences, journals, technical reports, etc.) it must be possible to be developed equivalent knowledge bases and demonstrate how the proposed solution enables the reuse and sharing of knowledge.

- **Practical Evaluation.** In this evaluation, the validity of the artefacts will be demonstrated in an organization to meet real needs. For that purpose, there is an agreement with a real organization that, for now, we will maintain anonym and identify as Organization for Validation (OfV). OfV is a government-owned organization in charge of providing goods and services to both public and private customers. As part of its management strategy, OfV ensures that all functions are performed according to the defined requirements and regulations and that risk is managed at all levels of the organization. The actual context of OfV can be characterized as an organization that has several domain-specific RM processes that were defined to meet operational needs (for example, the need for security certifications), or business needs (for example, to comply to a requirement of an international or national call). Those processes are responsible for the generation of the organization risk information that needs to be consolidated and harmonized by OfV competent department in order to produce a RM report to the strategic management of the organization. The process of consolidation and harmonization of risk information is recognized as difficult and time-consuming due to the heterogeneity of the generated risk information. Therefore, one of the OfV needs and goals is to define an ERM framework that will assure that all domain-specific RM processes follow common RM good practices without restricting the use of domain-specific concepts and techniques. The ERM framework
should also support the integration of risk information generated in those domain-specific processes. It is expected that the results of this work will support the definition of OfV ERM Framework. As of the moment of writing, we are still searching for other organizations with similar needs to support this practical evaluation.

Additionally, all relevant results of the research will be disseminated in conferences and journals. We plan to publish in 2 journals and in no less than 2 high-ranked conferences proceedings. Development will occur in two iterations. The first iteration already started and is planned to finish in June 2017 with the development of the first functional prototype of the solution. The first iteration will be revised according to the theoretical and practical evaluation leading to the second iteration planned to finish in September 2017. Finally, the conclusion, that implies the writing of the research work, is planned to last 8 months and will conclude in December 2017.

6 References


