Ontology-based Operational Risk Management

Ioanna Lykourentzou
Centre de Recherche Public Henri Tudor
Luxembourg, Luxembourg
Ioanna.Lykourentzou@tudor.lu

Katerina Papadaki
Bank of Greece
Athens, Greece
kpapadaki@bankofgreece.gr

Apostolis Kalliakmanis
University of Liverpool
Liverpool, United Kingdom
Kalliakmanis_Apostolis@emc.com

Younes Djaghloul
Centre de Recherche Public Henri Tudor
Luxembourg, Luxembourg
Younes.Djaghloul@tudor.lu

Thibaud Latour
Centre de Recherche Public Henri Tudor
Luxembourg, Luxembourg
Thibaud.Latour@tudor.lu

Ioannis Charalabis
National Technical University of Athens
Athens, Greece
i.haralampis@prv.ypeka.gr

Epaminondas Kapetanios
School of Computer Science, University of Westminster,
E.Kapetanios@westminster.ac.uk

***Abstract*—Operational risk management (ORM) is a process of critical importance to organizations. It refers to the systematic identification, assessment and mitigation of operational risks, i.e. risks stemming from processes, people, systems or external events. ORM is performed through different systems in the different business units of the enterprise – however a unified view of the operational risk management information is needed to enable its seamless exchange and horizontal expertise sharing. At the level of corporate governance this is already addressed but, at the technical level this issue is still open. As a solution in this paper we propose the development of an ORM ontology. The proposed ontology aims at facilitating ORM information sharing across organizational unit boundaries and at the enabling of computational inferences over the heterogeneous ORM applications of the organization.**

Operational Risk; Operational Risk Management; Ontologies

I. INTRODUCTION

Operational risk management is the entire process of continuously and systematically identifying, analyzing, responding to, reporting on and monitoring operational risks [1, 2]. In order to effectively share the risk management information it is necessary to have a common understanding regarding the risk management knowledge domain that will ensure a consistent view of the risks across the organization. At the corporate governance level this is addressed by the adoption an organization-wide operational risk management framework that will ensure a consistent view of the risks across the organization [3]. But at the technical level the operational risk information sharing issue also needs to be addressed.

As a solution to this issue this study proposes the creation of an operational risk management ontology. An ontology is a general conceptualization of a specific domain in both human and machine readable format. Thus, the proposed ontology will include the main concepts of the operational risk management knowledge domain, thus promoting a common understanding of operational risks and establishing a consistent risk management approach across the organization.

The proposed ontology is expected to address the issue of sharing operational risk management information across the organization thus promoting the collaboration between business areas regarding the common as well as the horizontal operational risks. Furthermore the proposed ontology will aid the operational risk management group in gathering heterogeneous information from all business areas and communicating it effectively to the enterprise management in order to support the decision making process the organization governance strategy regarding risks. Additionally the representation of the operational risk management ontology in semantic web languages will enable the computation and inference over information residing in heterogeneous risk management applications of the organization, leading to the emergence of operational risk knowledge that could not have been realized by the individual applications.

The rest of this paper is organized as follows: section 2 presents a review of the related research literature, section 3

Acknowledgements
This work was partially carried out during the tenure of an ERCIM "Alain Bensoussan" Fellowship Programme at the Centre de Recherche Public Henri Tudor, Luxembourg. The authors would also like to thank Dr Shakil Ahmed at the University of Liverpool for his valuable advice during the creation and evaluation of the ORM ontology.

provides an overview of the essential concepts of operational risks and operational risk management, section 4 presents the developed ontology and section 5 concludes with the main findings and future directions of this work.

II. Related Literature

The related literature presented in the following, is divided into three parts: a) the studies devoted to operational risk management, b) the background on ontology definitions and c) the related work in enterprise ontologies.

A. Operational risk management

Operational risk is defined as the risk of negative financial, business and/or reputation impacts resulting from inadequate or failed internal governance and business processes, people, systems, or from external events [3]. Operational risk management is the entire process of continuously and systematically identifying, analyzing, responding to, reporting on and monitoring operational risks [1, 2].

Operational risks occur throughout an institution, and the primary responsibility for management is in the business areas. Business areas perform self-assessments, collect event data, and measure and analyze risk drivers and indicators [4]. Although risks are managed across diverse businesses and risk types, senior management wants a consolidated view. The corporate operational risk management group's key role is to aggregate information from the business areas to inform senior management, conduct independent analyses of results and trends, and benchmark results, both across units internally and to external sources [5].

From the technical viewpoint, the various business areas use different information systems for the management of their operational risks. Due to the distributed, heterogeneous and autonomic characteristics, of these systems it is not easy for the operational risk management group to integrate them to provide a seamless communication of risk management knowledge [6, 7].

All these, and possibly other factors as well, have resulted in growing numbers of books, articles and conferences being devoted to operational risk management. Due to Basel Committee standard [3] that is obligatory for the banking sector and connects operational risk with capital requirements there are many articles on the quantitative operational risk management methods (e.g. AMA). Despite the interest in risk management in the industry, very little academic research has been conducted to provide a better understanding of how operational risk management can be improved within organizations. As a result a relatively small number of operational risk management articles are published in peer-reviewed academic journals. In their survey on academic research on risk management in enterprises, [8], attribute the shortage of such articles mainly to the lack of a foundational framework, which makes it impossible to build from prior research. Another factor that limits this research is that organizations are reluctant to reveal information about their risk management practices.

Nevertheless, recently a paper was published on the correlation between risk management quality and risk knowledge sharing [9], based on a questionnaire survey of risk management employees. This research indicated the importance of improving risk information sharing within organizations. Therefore the present paper contributes towards increasing risk information sharing through the creation of the ORM ontology.

B. Ontology definitions

The term "ontology" originating from philosophy, has been given plenty of definitions in computer-science [10]. For the needs of this paper the definition that better describes the case of the operational risk ontology is the following: *"an ontology defines the basic terms and relations that compose the dictionary of the field of interest and the rules that combine the terms and relations so that the dictionary of terms is extended" [10]*. The description of ontology in the field of interest includes the most important meanings, (the classes or concepts), the properties (or slots/roles) and the properties restrictions (or facets) [11]. The ontology and the instances of the relative classes compose a knowledge database. Often, the boundaries between ontology and this database are not clearly distinguished.

Ontologies can be modeled by many techniques and expressed in many languages. They are divided in two categories: the highly informal if they are expressed in natural language and in semi-informal if they are expressed in a structure form of nature language, in semiformal if they are expressed in a technical and formally defined language as the OWL Ontology Language [12] and in firmly formal if they include absolute semantic terms, theories and proofs [13]. According to this discrimination, the operational risk management ontology that is presented in this paper is a semiformal ontology expressed in OWL

C. Enterprise ontologies

There are many ontology categorizations [14, 15]. By following the categorisation of Mizoguchi and his collaborators in this paper the ontology of operational risks is considered to belong in the category of Domain Ontologies, subclass Enterprise Ontologies [14, 16]. Most widely known in this category are the Enterprise Ontology (Uschold et al, 1998) and TOVE (Toronto Virtual Enterprise) ontology (Fox, 1992).

In the category of enterprise ontologies is included also a frame of ontologies known as Semantic Business Process Management (SBPM) [17], which attempt the complete corresponding of all processes of an organisation, from the administrative until the functional level. BusCo [18] is also an enterprise ontology, which attempts its differentiation from existing enterprise ontologies on issues such as the degree of analysis of significances, the description of resources of an organisation, the significance of organisational memory and the measurement of performance. The determination of risks and opportunities in strategy level is the objective of another research effort called STRATrisk [19].

Apart from the enterprise ontologies there has been development of ontologies that focus in concrete risk categories such information systems security risks, for which

one may find extensive reviews [20], as well as complete approaches and applications to support the decision-making for the reduction of risks [21]. In addition, ontologies have been proposed that specialize the requirements of information security for specific domains such as electronic governance [22] and the electronic services of health [23]. An ontology has also been developed for managing the technological risks in enterprises of the banking sector [24].

Studying the above literature, it is understandable that there are quite developed enterprise ontologies that appear to have the following drawbacks:

- They examine the risks in the level of enterprise strategy and not in the level of procedures, meaning that they have a top-down approach, which is not combined with an approach in lower level, i.e. the bottom up approach.
- Even though some of these ontologies include the concept of process very often in the high level of detail, they don't incorporate elements of operational risk management in the level of processes.
- They focus on very specific risk categories (for instance on security) and they don't cover other operational risk categories.
- They focus on risks of particular enterprise fields (such as the banking sector) resulting in not giving the ability of generalizing in other sectors.

In relation with the existing enterprise ontologies the ontology proposed in this paper should:

- Be enough general so that it can be suitable for a big number of enterprise units.
- Focus on enterprise processes and
- Cover all the categories of operational risk in the organizational processes of each business unit.

By this way, ontology will contribute in the improvement of the enterprise ontologies and in the more efficient operational risk management.

III. OPERATIONAL RISK MANAGEMENT CONCEPTS

A. *Definition of Operational Risk*

Operational risk is defined as the risk of negative impacts on the economic situation, in the operation and / or validity of an organization as a result of inadequacy or failure of:

- Internal Governance, and processes
- People,
- Systems, or
- As result of external events [3]:

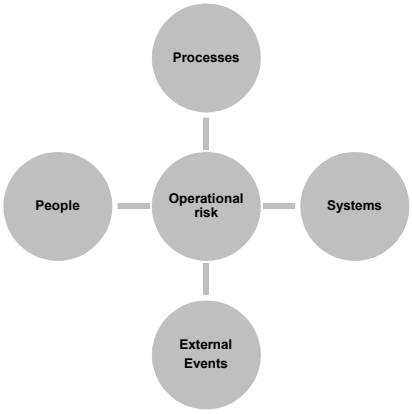

Figure 1. Operational Risk

B. *Operational Risk Management*

Operational risk management is an important element of governance and administration, which aims to protect an organization from internal and external environment risks, which will negatively affect the operational targets of the organization. Operational risk management is characterized by its focus on business processes. Operational risk management in an organization tries to predict and prevent any event which could cause a failure in the achievement of operational procedures. Examples of such events are human errors, failures of systems or even external attacks.

Operational risk management is a constant and systematic process which consists of the following stages (Figure 2) [25]:

- Risk identification
- Risk assessment
- Risk treatment
- Risk report and monitoring

Risk management is an iterative process that must be performed firstly top-down, i.e. at a high level, in order to identify the key risks, and at the bottom-up, i.e. at a low level, to identify all risks in more detail. In both approaches the same steps are followed in the process of risk management, and the difference lies in the degree of thoroughness.

Figure 2. Operational Risk

C. Operational Risk Management Process

Below, the steps of the operational risk management process are described:

Risk Identification: This step includes the identification of the major risk events that may negatively impact the performance of processes and of the organization in general. All the recognized risks must be properly documented. The documentation of risks includes the brief description of the risks, a clear definition of their root causes, information regarding real available incidents, as well as a review of the control environment or a list of existing checks.

Risk Assessment: For each risk that has been identified at the previous step the following activities take place:

- Evaluation of the effectiveness of the existing controls/measures.
- Assessment and documentation of the likelihood of occurrence of the operational risk event, using a predefined scale rating the likelihood of realization.
- Assessment and documentation of the impact of operational risk event, using predefined scale of rating the impact.

Also, at this point, the concept of the risk tolerance policy should be presented. This policy defines whether an individual risk needs to be treated or whether certain risks need to be accepted, mainly in case that their treatment is too expensive for the organization [1].

IV. Operational Risk Management ontology: Methods and Realization

A. Ontology development methodology

The process of ontology development and evolution has been studied in the ontology engineering context [26] and many methods have been proposed such as the CYC, the Uschold and King, the Gruninger and Fox, the KACTUS, METHOLOGY, SENSUS and On-To-Knowledge method [13]. For the particular requirements of operational risk management ontology development a methodology was selected which was proposed by Mizen, Dolbear and Hart [27]. This methodology has been established from 2004 as a standard methodology for the creation of risk management ontologies and has been applied for the development of risk management ontologies for natural catastrophes. Furthermore an important reason for the selection of this methodology is the fact that it makes the distinction between the conceptual and the logical part of an ontology, i.e. the high-level, human-understandable part and the part that is intended to be processed by information systems.

Thus, the methodology stages for the conceptual ontology development are the following:

Stage 1: Collection of the necessary data and definition of the ontology requirements

Stage 2: Creation of a glossary of the basic concepts.

Stage 3: Creation of the concept network, by connecting concepts based on their in-between relations.

Stage 4: Assessment/evaluation of the conceptual ontology.

Stage 1: Data collection and requirements definition

The data collection regarding the concepts that are included in the operational risk ontology is based on the international risk management standards, mainly [25, 28, 29] and risk management methodologies [30].

For the definition of the requirements and the data collection of the ontology at this point of the development methodology it is very helpful to pose certain questions that will be answered when using the ontology. These questions are known as competency questions [16].

Some of the competency questions of the operational risk ontology might concern the detail of the risk description:

- Which are the risks of a specific process?
- What's the likelihood of a risk to occur?
- How serious can the consequences of this risk be for the organization if this risk occurs?
- What is the root cause of the risk's occurrence?
- What is the way of treating the risk?

Also, questions about all the risks should be answered. For instance:

- How many high risks have been identified in the whole organization?
- Which are the processes that are affected by these risks?
- What risks are provoked by a particular root cause?

In order to be able to give answers to these questions operational risk ontology should include all the characteristics of a risk and give the opportunity of extracting information and categorizing all the risks according to these characteristics. The data that were collected at this stage are presented in the next paragraph.

Stage 2: Glossary of concepts

Based on the data that collected at the previous stages of the development methodology, the basic concepts and relations between them for the operational risk management were defined. These are presented briefly in the following:

1. **Process**: The procedures that are performed within an organization. A process is described by characteristics as: in which operational unit it belongs, which kind of resources it requires, by which activities is consisted of, by which processes it collects input data, to which processes it provides output data etc.

In the context of the operational risk ontology this class has not been specified in detail, mainly because this is not be part of risk management but a part of the enterprise business process management, and secondly because such an attempt would overlap with the already existing enterprise ontologies [16, 18] we have referred to in the related literature section.

2. **ProcessRisk**: The most important concept of the ontology. It refers to a risk of a process (a process usually has many risks). ProcessRisk concept is significant for all the risk management stages. In the following, other concepts used to characterize a risk are described.

3. **Impact**: The level of consequences of a risk. This concept is very significant for the risk assessment. With the aim of presenting the different levels of impacts of a risk we

have created 3 subclasses: HighImpact, MediumImpact and LowImpact, which correspond to 3 rates of impact.

4. **Likelihood**: The possibility for a risk to happen. This concept is crucial for the risk assessment. As in the Impact class, we also here create 3 subclasses: HighLikelihood, MediumLikelihood and LowLikelihood.

5. **RiskEvent**: The taxonomy of the risk events. This concept is important for the stage of risk identification during the operational risk management process. In the specific ontology we chose the creation of 7 subclasses: Errors or Failures, Infrastructure disruption, Occupational incidents, Frauds, Disasters, Attacks and Other events.

6. **RiskRootCause**: The taxonomy of the initial causes of the risks and is divided in four subclasses in the first level: (1) People, (2) Governance and business process, (3) Systems and (4) External Events. The creation of 4 subclasses is in accordance with the definition of operational risk. Each one of the subclasses can be analyzed in more levels depending on the detail level we desire to include in our risk root cause analysis. This root cause taxonomy is useful in the stage of planning the actions of treating the risks.

7. **TreatmentPlan**: The action plans of treating risks.

8. **Incident**: Real incidents of risks. This concept is crucial for the risk monitoring.

In the following, we will describe the properties of the ontology classes. These properties could be object properties or data properties. The first one, the object property can relate members of a class indicating a relationship between them. The second one, the data property connects the member of a class with a value.

9. **belongsToProcess**: Data property. It represents the relationship between the class ProcessRisk and the class Process. It symbolizes the fact that a risk is related to a specific process. According to the approach we have adopted in the specific risk ontology, due to the fact that a risk belongs to only one process, the property belongsToProcess is functional.

10. **hasRisk**: Object property. It is inverse of the belongsToProcess and connects the classes of the Process Risk and the process. The property hasRisk is not functional because a process may have many risks.

11. **hasImpact**: Object property. It describes the relationship between the class ProcessRisk and the class Impact. It is functional and characterized by a specific level of impacts.

12. **hasLikelihood**: Object property. It describes the relationship between the class ProcessRisk and the class Likelihood. It is functional because a risk is characterized by only one likelihood of occurrence.

13. **isResultOf**: Object property. It describes the relationship between the class ProcessRisk and the class RiskEvent. Even if a risk could theoretically be a result of many events, in this approach we accept that a risk is a result of one event, so the property is functional.

14. **hasRootCause**: Object property. It describes the relationship between the class of ProcessRisk and the class of RiskRootCause. Even if a risk could be a result of several initial causes, in this approach we assume that the risk has one initial RootCause so the property is functional.

15. **hasTreamentPlan**: Object property. It describes the relationship between the class of ProcessRisk and the class of TreatmentPlan. This is not a functional property as there can be more than one treatment plans for a risk.

16. **hasIncident**: Object property. It describes the relationship between the class of ProcessRisk and the class of RiskEvent. This is not a functional property as there can be more than one event for a risk.

Stage 3: Conceptual network of the ORM ontology

The conceptual network operational risk ontology based on the information gathered in the previous section for the concepts/classes and relations/properties and is depicted in Figure 3.

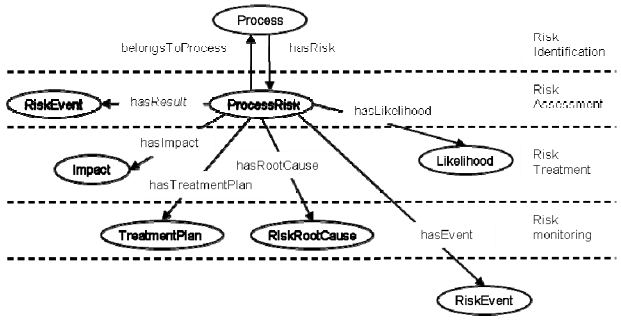

Figure 3. Conceptual network of operational risk ontology

Stage 4: Assessment/evaluation

In the context of this paper, the objective was to evaluate the conceptual ORM ontology, in order to identify strengths and weaknesses with a view to further improve the ORM ontology. Thus, the ORM ontology was evaluated on the basis of two main dimensions: a) ontology content and b) ORM specific capabilities.

The evaluation methods used were two: (i) structured interviews with questionnaire and (ii) performance of tasks and observation.

The participants that evaluated the ORM ontology are 10 information technology experts from academia and industry. The validity of the evaluation results was ensured by the strong academic and professional background of the participants and also by their involvement in different business and academic environments. The detailed design of the evaluation procedures and instruments (questionnaire and tasks) added validity to the process.

Additionally in the design phase of the evaluation the evaluation protocol was reviewed by an expert in empirical research.

In the following we present and discuss the results of the aforementioned evaluation.

Dimension: Content

The purpose of this evaluation dimension was to examine the usefulness and completeness of the ORM ontology content. Four content factors were examined:

1. Concepts
2. Relations

3. Taxonomy
4. Axioms

As it may be observed in Figure 4, the average ratings for the above factors of the ontology content dimension ranged from 1.4 to 4.6 and the standard deviation ranged from 0.5 to 0.8, which gives an overall positive rate for the ontology content. The average of 1.4 for the factor axioms is attributed to the fact that essentially the ORM ontology contains no axioms at this point.

Evaluation result: The content of the ORM ontology was rated positively by the participants regarding the concepts, their relations and the taxonomy. The participants expressed the opinion that the ORM ontology contains all the necessary concepts, relations and taxonomies required for performing all the ORM tasks, in a simple and yet complete approach. The absence of axioms at this point was not considered to affect the ontology, although should be addressed in the future. Taking into consideration that it was a prototype, the participants indicated that in future versions the ORM ontology has to be enriched with concepts that will act as links with other domain ontologies.

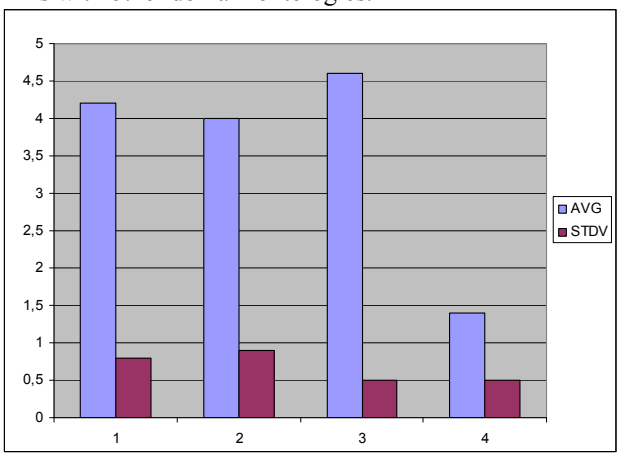

Figure 4. Average and Standard Deviation for the Factors of Dimension: Ontology Content

Dimension: ORM specific capabilities

This dimension examined the capabilities of the ontology in serving more specific needs of the ORM process. In this context, the following four content factors were examined:

1. Coverage of all RM phases
2. Facilitation of self assessment
3. Appropriateness for all organizational levels
4. Connection with other domain ontologies

As it may be observed in Figure 5, the average ratings for the factors of ORM Specific Capabilities dimension ranged from 2.9 to 4.3 and the standard deviation ranged from 0.8 to 1, which gives an overall good rate for the ORM Specific Capabilities. The average of 2.9 for the factor 4: Connection with other domain ontologies was discussed with the participants. This low rate, relatively to the other factors of this dimension, is attributed to the fact that in its current status the ORM ontology is connected to the Process ontology in a rather implicit way. In the future this connection and also connections to other business ontologies, such as for example a business continuity ontology should be made more explicit. The standard deviation of 1 in the factor: Appropriate for all Organisational Levels indicates that this issue should be further researched and assess the cost of adding the necessary functionalities versus the benefit of making the ORM ontology appropriate to all organisation levels. Nevertheless, the ORM ontology was created with the objective to be useful primarily to the ORM unit of an organisation. The fact that this unit supports all the organisational levels of the organisation makes the ORM ontology indirectly useful to all the organisation.

Evaluation result: The ORM specific capabilities of the prototype were generally appreciated by the participants. In particular it was considered appropriate for the facilitation of self-assessment by the organisation units for ORM, because of its simplicity and completeness as it covers all risk management phases. It was also thought as being very useful for the specialised risk management units, since it helps though reasoning and inference capabilities to categorise the risk information from organisational units and create meaningful reports for the top management. Therefore, regarding the top management of the organisation the use of the ORM ontology is considered to be very useful but rather indirectly through the consolidated reports created by the risk management unit. A very important feature that looks very promising for the organisation as a whole, but will become more apparent in the future versions of the ORM ontology, is the connection with other enterprise ontologies with concepts related to corporate governance, like to business processes management, business continuity and audit.

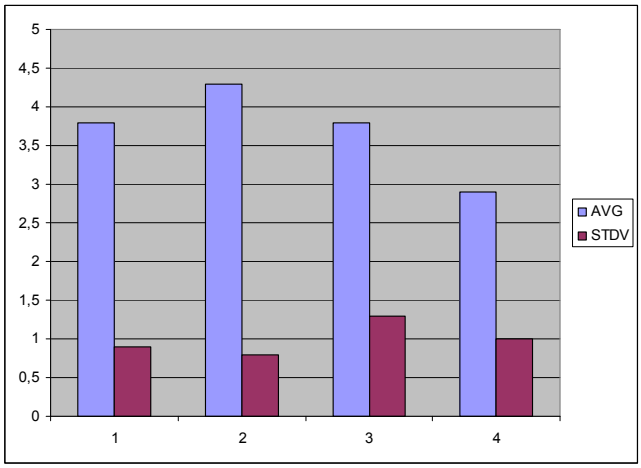

Figure 5. Average and Standard Deviation for the Factors of Dimension: ORM Specific Capabilities

B. Logical Operational Risk Ontology

In the following, we present the representation of the ontology based on the syntax of description logic.

Process := ∃*belongsToProcess*. ProcessRisk ∩ ≥1 *hasRisk*. ProcessRisk

ProcessRisk := ∃*hasImpact*. Impact ∩ ∃*hasLikelihood*. Likelihood ∩ ∃*isResultOf*. RiskEvent ∩ ∃*hasRootCause*. RiskRootCause ∩ ≥1 *hasTreamentPlan*.TreatmentPlan ∩ ≥1 *hasIncident*.Incident

High impact ⊆ Impact
Medium impact ⊆ Impact
Low Impact ⊆ Impact

High Likelihood ⊆ Likelihood
Medium Likelihood ⊆ Likelihood
Low Likelihood ⊆ Likelihood

Errors or failure ⊆ RiskRootCause
Infrastructure disruption ⊆ RiskRootCause
Attacks ⊆ RiskRootCause
Occupational incidents ⊆ RiskRootCause
Frauds ⊆ RiskRootCause
Disasters ⊆ RiskRootCause
Other events ⊆ RiskRootCause

People ⊆ RiskRootCause
Governance and business Processes ⊆ RiskRootCause
Systems ⊆ RiskRootCause
External Events ⊆ RiskRootCause

V. Conclusion and Future Work

In this paper, we present our initial work on the research issue of developing an ontology to serve the needs of the Operational Risk Management (ORM) business function.

The proposed ontology targets at facilitating the diffusion of operational risk-related information across the different divisions of the organization, as well as at helping the communication and data sharing among the different ORM computational applications used within the enterprise. The paper includes a brief description of operational risk and the ORM process, the developed ontology from a conceptual and a logical perspective.

Initial evaluation results, obtained through interviews with IT experts from academia and industry indicate that the developed ontology contains the necessary concepts and relations required to perform the necessary ORM tasks, while it was also considered appropriate for the facilitation of ORM self-assessment performed by the different organizational units.

Future work will include an identification and definition of more relationships among the six main classes of the ontology, as well as its further fine-graining regarding specialized ORM corporate needs.

References

[1] CSOTC, "Enterprise Risk Management-Integrated Framework," *Book Enterprise Risk Management-Integrated Framework*, Series Enterprise Risk Management-Integrated Framework, Committee of Sponsoring Organisations of the Treadway Commission, 2004.

[2] G. Koller, *Risk Assessment and Decision Making in Business and Industry*, CRC Press 1999.

[3] BCBS, "Sound Practices for the Management and Supervision of Operational Risk," *Book Sound Practices for the Management and Supervision of Operational Risk*, Series Sound Practices for the Management and Supervision of Operational Risk, Basel Committee on Banking Supervision, 2003.

[4] J. Sabatini and M. Haubenstock, "OR: management reporting of operational risk; a series designed to introduce readers to the tools used in the management of operational risk in today's financial services industry," *The RMA Journal*, May 1, 2011 2002; http://findarticles.com/p/articles/mi_m0ITW/is_10_84/ai_n14897145.

[5] P. Collier, *Risk Evaluation, Treatment and Reporting, In: Fundamentals of Risk Management for Accountants and Managers*, Butterworth-Heinemann, 2009.

[6] R.J. Chapman, *Simple tools and techniques for enterprise risk management*, John Wiley & Sons 2006.

[7] F. Sallmann, *Knowledge-based risk management*, VDM Verlag 2007.

[8] S.R. Iyer, et al., "Academic Research on Enterprise Risk Management," *Enterprise Risk Management*, J. F. a. B. S. (Eds), ed., Wiley, 2010.

[9] E. Rodriguez and J. Edwards, "People, Technology, Processes and Risk Knowledge Sharing," *Electronic Journal of Knowledge Management* vol. 8, no. 1, 2010, pp. 139-150.

[10] R. Neches, et al., "Enabling technology for knowledge sharing " *AI Magazine* vol. 12, no. 3, 1991, pp. 36-56.

[11] N. Noy, F. and D. McGuinness, L., *Ontology Development 101: A Guide to Creating Your First Ontology*, Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, 2001.

[12] S. Bechhofer, et al., "OWL Web Ontology Language Reference," *Book OWL Web Ontology Language Reference*, Series OWL Web Ontology Language Reference, 2004.

[13] A. Gómez-Pérez, et al., *Ontological Engineering*, Springer, 2004.

[14] O. Lassila and D. McGuiness, *The Role of Frame-Based Representation on the Semantic Web*, Technical Report, Knowledge Systems Laboratory, Stanford University, KSL 01-02, 2001.

[15] v. Heist, G., et al., "Using Explicit Ontologies in KBS " *International Journal of Human-Computer Studies* vol. 46, no. 2, 1997, pp. 183-292.

[16] P. Rittgen, *Handbook of Ontologies for Business Interaction*, IGI, 2008.

[17] M. Hepp and D. Roman, "An Ontology Framework for Semantic Business Process Management," *Proc. 8th International Conference Wirtschaftsinformatik 2007*, 2007, pp. 423-440.

[18] Y. Jussupova-Mariethoz and A. Probst, "Business concepts ontology for an enterprise performance and competences monitoring," *Comput. Ind.* , vol. 58, no. 2, 2007, pp. 118-129.

[19] G.M. Allan, et al., "Risk Mining for Strategic Decision Making," *Proc. Adv. in Intel. Web ASC 43*, 2007, pp. 21-28.

[20] C. Blanco, et al., "A Systematic Review and Comparison of Security Ontologies," *Proc. In Proceedings of the 2008 Third international Conference on Availability, Reliability and Security*, 2008, pp. 813-820.

[21] A. Ekelhart, et al., "Automated Risk and Utility Management," *Proc. In Proceedings of the 2009 Sixth International Conference on Information Technology: New Generations*, 2009, pp. 393-398.

[22] M. Karyda, et al., "An ontology for secure e-government applications," *Proc. Proceedings of the First International Conference on Availability, Reliability and Security (ARES)*, 2006 pp. 20-22

[23] S. Dritsas, et al., "A knowledge-based approach to security requirements for e-health applications," *The electronic Journal for E-Commerce Tools & Applications eJETA*2006; http://www.ejeta.org/specialOct06-issue/ejeta-special-06oct-4.pdf.

[24] C. Atkinson, et al., "Concepts for an Ontology-centric Technology Risk Management Architecture in the Banking Industry," *Book Concepts for an Ontology-centric Technology Risk Management Architecture in the Banking Industry*, Series Concepts for an Ontology-centric Technology Risk Management Architecture in the Banking Industry, 2006

[25] I. IEC, "ISO/FDIS 31000 Risk management-Principles and guidelines," *Book ISO/FDIS 31000 Risk management-Principles and guidelines*, Series ISO/FDIS 31000 Risk management-Principles and guidelines, 2009.

[26] P. De Leenheer and T. Mens, *Ontology evolution State of the Art and Future Directions*, Springer, 2008.

[27] H. Mizen, et al., *Ontology Ontogeny: Understanding How an Ontology is Created and Developed*, Springer, 2005.

[28] S. Australia, "AS/NZS 4360:2004 Australian/New Zealand Standard for Risk Management," *Book AS/NZS 4360:2004 Australian/New Zealand Standard for Risk Management*, Series AS/NZS 4360:2004 Australian/New Zealand Standard for Risk Management, 2004.

[29] AIRMIC, "ALARM, IRM, A Risk Management Standard," *Book ALARM, IRM, A Risk Management Standard*, Series ALARM, IRM, A Risk Management Standard, 2002.

[30] ENISA, "Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools," *Book Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*, Series Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, 2006.