A Common Terminology for Software Risk Management

Jhon Masso*

Alarcos Research Group, Institute of Technologies and Information Systems, University of Castilla-La Mancha, Spain and GTI Research Group. Electronic and Telecommunications Engineering Faculty, University of Cauca, Colombia, masso@unicauca.edu.co

Félix García

Alarcos Research Group, Institute of Technologies and Information Systems, University of Castilla-La Mancha, Spain, felix.garcia@uclm.es

César Pardo

GTI Research Group. Electronic and Telecommunications Engineering Faculty, University of Cauca, Colombia, cpardo@unicauca.edu.co

Francisco J. Pino

IDIS Research Group. Electronic and Telecommunications Engineering Faculty, University of Cauca, Colombia, fjpino@unicauca.edu.co

Mario Piattini

Alarcos Research Group, Institute of Technologies and Information Systems, University of Castilla-La Mancha, Spain, mario.piattini@uclm.es

In order to improve and sustain their competitiveness over time, organisations nowadays need to undertake different initiatives to adopt frameworks, models and standards that will allow them to align and improve their business processes. In spite of these efforts, organisations may still encounter governance and management problems. This is where Risk Management (RM) can play a major role, since its purpose is to contribute to the creation and preservation of value in the context of the organisation's processes. RM is a complex and subjective activity that requires experience and a high level of knowledge about risks, and it is for this reason that standardisation institutions and researchers have made great efforts to define initiatives to overcome these challenges. However, the RM field nevertheless presents a lack of uniformity in its terms and concepts, due to the different contexts and scopes of application, a situation that can generate ambiguities and misunderstandings. To address these issues, this paper aims to present an ontology called SRMO (Software Risk Management Ontology), which seeks to unify the terms and concepts associated with RM and provide an integrated and holistic view of risk. In doing so, the Pipeline framework has been applied in order to assure and verify the quality of the proposed ontology, and it has been implemented in Protégé and validated by means of competency questions. Three application scenarios of this ontology demonstrating their usefulness in the software engineering field are presented in this paper. We believe that this ontology can be useful for organisations that are interested in: (i) establishing an RM strategy from an integrated approach, (ii) defining the elements that help to identify risks and the criteria that support decision-making in risk assessment, and (iii) helping the involved stakeholders during the process of risk management.

CCS CONCEPTS • Software and its engineering ~Software creation and management ~Software development process management ~Risk management

Additional Keywords and Phrases: Risk Management, Integrated Risk Management, Risk Ontology, ISO 31000

1049-331X/2022/1-ART1 $15.00
http://dx.doi.org/10.1145/3498539

1 INTRODUCTION

Nowadays, software organisations use different management approaches to improve the success of their projects and optimise their processes [47]. This has led to great efforts and changes in these organisations, in an attempt to adapt to the new business environments and thus respond quickly and accurately to current markets [38], and has led to an evolution and transformation in the organisational structure and culture [107].

However, despite these efforts, organisations - whatever their size and field [22,133] - are still exposed to various types of risks that threaten their organisational and operational structure. Many of these risks are sometimes difficult to identify, leaving organisations deeply uncertain as to when they might occur and how to respond correctly [122]. This is where Risk Management (RM) becomes a key challenge for most organisations, as it requires a well-defined process that is aligned with the organisation's objectives [8]. In addition, it requires organisations to pay careful attention, as RM can contribute to reduce risks in business processes, financial losses, damage to the reputation or image of the business, etc. [125]. Risks therefore reflect both opportunities for profit and threats to success [57] and not addressing them could lead to a reduction in an organisation's market share [110]. All this makes RM a key strategic activity that could help towards the success of the business [57].

As a result, organisations make great efforts in taking decisions on the selection and adoption of approaches that will best suit their needs and effectively manage risks [112]. However, they are then faced with a wide variety of RM approaches, which are defined by standardisation institutions and researchers, making it more difficult to choose the most appropriate one [112]. Many of these have been developed for specific contexts or sectors of application and to meet diverse needs [3] (e.g., corporate, project, information security, IT services, etc.). On the other hand, organisations often use different RM approaches and practices, with the result that RM is not done systematically [108]. The application of diverse RM proposals involves a lack of consistency in the terminology associated with risks [12], where different terms can be used without a clear and coherent semantics, and this could lead to a deficient understanding of RM activities and therefore to a poor implementation [27].

To address the aforementioned issues, this paper proposes a domain ontology called SRMO which aims to help reduce the ambiguity of the terms and concepts associated with the RM domain. This ontology provides the key elements to support the definition and establishment of a risk management strategy (RMS) based on an integrated approach, which enables organisations to have a holistic view of risks. This is known in practice as integrated risk management (IRM). In other words, a form of risk management that "addresses risks across a variety of levels in the organisation, including strategy and tactics, and covering both opportunity and threat" [20]. In addition, it provides a multidimensional view of risk that helps to identify and evaluate the effects that risks have on the value of the company. This is achieved through a coherent and organised approach, which enables the implementation of an RMS at all levels of the organisation, instead of a traditional or tactical implementation with a limited scope [85], [84]. RM, therefore, should not be carried out in isolation, but instead integrated into all structures and decision-making processes and should be linked directly to the achievement of objectives at all levels, since an RM that does not aid in decision-making may end up being simply ignored [127].

The SRMO derives from the analysis, comparison and integration of the terminology associated with RM contained in different standards, frameworks and models widely recognised by the industry such as ISO 31000, COBIT, PMBOK and CMMI. This ontology facilitates the definition of elements that will enable the identification of the different sources and risk factors that may affect the organisation's assets. It also establishes the risk criteria that will support the decision-making process during the risk assessment process. Furthermore, it provides support to interested parties during the RM process, to carry out an adequate management of all the information related to risks. SRMO is a generic

ontology, independent of an RM approach, which can be employed by any type of organisation and applied in the context of the software life cycle.

The remainder of this paper is organised as follows. Section 2 discusses the background to this research and the analysis of related research, plus the conceptual premises used for the development of this proposal. In Section 3, the issue of ontologies, and the methodology adopted for the elaboration of this proposal, is described. Section 4 presents a common ontology for software RM that provides for the harmonisation of the terminology and concepts associated with this domain, along with the description of its implementation. Then, an evaluation of the ontology and the popularisation of its results is presented in Section 5. A general discussion about the contributions of this ontology is contained in Section 6. Finally, the conclusions are presented in Section 7.

2 BACKGROUND

2.1 Risk management in main standards & frameworks

Nowadays, at a business level, there is an outstanding use of standards, management and governance frameworks that encompass RM and that are intended to help achieve the goals and objectives of the organisation, as well as to guide professionals in obtaining good results and gaining an awareness of this management practice. Some of the standards most widely used and recognised by the industry as good practices are ISO 31000, COBIT, PMBOK and CMMI [9,21,22,37,100,132]. A summary of the main characteristics of each of these approaches that support RM is shown in Table 1.

Table 1: Summary of the approaches that support risk management

Characteristic	Approach			
	ISO 31000:2018	COBIT 2019	PMBOK® Guide – 6th Ed	CMMI V 2.0
Name	Risk management - Guidelines	Objectives for Information and Related Technology	Project Management Body of Knowledge	Capability Maturity Model Integration
Organisation Developer	ISO – International Organisation for Standardisation	Information Systems Audit and Control Association (ISACA)	Project Management Institute (PMI)	CMMI® Institute an ISACA Enterprise
Version	2018	2018	2017	2018
Application Domain	Overall	Governance of enterprise IT (GEIT)	Projects	Development, Services, Supply management and People management
Organisational Certification	N/A	N/A	N/A	Yes
RM Processes or practices	1 Processes and 6 major subclauses: 6.2 communication and consultation 6.3 scope, context, criteria 6.4 Risk Assessment 6.4.2 Risk identification 6.4.3 Risk analysis 6.4.4 Risk evaluation 6.5 Risk treatment 6.5 Monitoring and review 6.6 Recording and reporting	2 Processes (EDM03 and APO12) and 9 practices. EDM03 Risk Optimisation: EDM03.01 Evaluate risk management EDM03.02 Direct risk management EDM03.03 Monitor risk management APO12 Manage Risk: APO12.01 Collect data, APO12.02 Analyse risk APO12.03 Maintain a risk profile APO12.04 Articulate risk APO12.05 Define a risk management action portfolio APO12.06 Respond to risk	1 knowledge area (11- Project Risk Management) and 7 processes: 11.1 Plan Risk Management 11.2 Identify Risks, 11.3 Perform Qualitative Risk Analysis 11.4 Perform Quantitative Risk Analysis 11.5 Plan Risk Responses 11.6 Implement Risk Responses 11.7 Monitor Risks	1 practice Area (Risk and Opportunity Management - RSK) and 8 practices: RSK 1.1 Identify and record risks or opportunities and keep them updated RSK 2.1 Analyse identified risks or opportunities RSK 2.2 Monitor identified risks or opportunities and communicate status to affected stakeholders RSK 3.1 Identify and use risk or opportunity categories RSK 3.2 Define and use parameters for risk or opportunity analysis and handling RSK 3.3 Develop and keep updated a risk or opportunity management strategy RSK 3.4 Develop and keep updated risk or opportunity management plans RSK 3.5 Manage risks or opportunities by implementing planned risk or opportunity management activities.
Support to IRM	Yes	Yes	N/A (this is possible through [105])	Yes

RM Tools	N/A	N/A	Yes	Yes (implicit in the document itself)
RM Techniques	Yes (through ISO 31010 [67])	N/A	Yes	Yes (implicit in the document itself)
RM Metrics	N/A	Yes	N/A	N/A
RM Goals	N/A	Yes	Yes	N/A
Artefacts/Work Products	N/A	Yes	Yes	Yes
Capability Level	N/A	Yes	N/A	Yes
Roles and Responsibilities	N/A	Yes	N/A	N/A

Abbreviations - N/A: not applicable.

ISO 31000 was considered as it is the international standard designed to carry out the implementation of risk management in any type of organisation. Finally, it is important to note that one of the most relevant aspects for the choice of COBIT, PMBOK and CMMI is that they are focused on process management and project management, address and integrate RM within their structure and can be applied in software organisations.

2.1.1 ISO 31000.

ISO 31000:2018 is an international standard that establishes the common principles and guidelines for conducting RM, independently of the scope, organisation type, nature or consequences (positive/negative) of the risk [26,71,81,108]. Furthermore, it is a major reference for carrying out RM from a holistic viewpoint [7] and applies to any activity of the organisation [71]. ISO 31000 is based on three fundamental components or pillars: the principles, the framework and the RM process [71,76,121]. The principles are fundamental for the establishment of an RMS that enables the creation and protection of value in terms of the achievement of an organisation's objectives [71,95]. The framework is intended to assist the organisation in the integrated adoption of RM in all its processes, operational and governance activities [71]. The RM process is an iterative process that can be adapted and carried out in any organisation and applied at strategic, operational, program or project level to add value to the organisation and to assist stakeholders in making decisions and achieving objectives [71,112].

2.1.2 COBIT 2019.

COBIT 2019 is a framework for carrying out an effective Information and Technology (I&T) governance and management [55]. It is the best known and the most adopted framework in the industry [74,133]. It incorporates best practices for the design, implementation, monitoring, continuous improvement [56] and assurance of information technology (IT) [74]. COBIT is aimed at designing and implementing governance systems that are more flexible and personalised, that incorporate new technologies, and that are aligned with the main standards, frameworks and regulations related to this domain. In addition, it supports a CMMI-based scheme to determine the maturity and capability levels of the processes [55,56]. COBIT focuses on creating value from information and technology, optimising risk and resources [55]. Risk optimisation is a key objective in the preservation of value. Thus, as in COBIT, RM plays an important role and it is advisable to integrate it into the overall IT governance and management. It should also be measured to verify its impact and contribution to risk identification and management [52,56]. All of this is aimed at creating a culture that enables these practices to be sustained at all levels of the organisation in an effective and efficient manner, involving management, risk professionals and other members of the organisation [52]. ISACA has recently published a specific RM framework (Risk IT [57]) that facilitates the implementation of the controls defined in COBIT for governance and RM, through a structured methodology that enables the management and understanding of the risks related to IT at each level of the organisation.

2.1.3 A Guide to the Project Management Body of Knowledge (PMBOK).

PMBOK is a guide which provides the essential foundations for carrying out project management, and which includes a set of traditional and innovative practices that are widely used and tested in the PM profession [104]. In addition, this guide provides the tools and techniques that support project management activities in an organisation [15,134]. Project risk management is considered in PMBOK as a knowledge area whose objectives are "to increase the probability and/or impact of positive risks and to decrease the probability and/or impact of negative risks, in order to optimise the chances of project success" [104].

In addition, organisations working with the PMI philosophy through portfolios, programs and projects, can complement their management practices and especially their risk management practices with other standards, such as those defined in [105], which aim at integrating RM in the context of enterprise risk management, providing the essential components of RM in the different governance layers of portfolios, programs and projects. This is made possible through a framework that aims to create and maintain value through RM activities in the different domains of the organisation (enterprise, portfolios, programs and projects).

2.1.4 Capability Maturity Model Integration (CMMI V 2.0).

CMMI V2.0 is an integrated model of best practices designed for any business environment to build, maintain and improve the capability of the key business processes [17]. CMMI enables organisations to maintain and improve the execution of their processes in order to increase their quality, profitability and competitiveness [18]. This model is made up of development, service and supplier management views (views considered as constellations in version 1.3 [109]). RM in this model is considered a practical area which is called Risk & Opportunity Management (RSK). RSK is intended to identify, record, analyse and manage potential risks and opportunities that may occur at the project level, in order to mitigate negative effects or harness positive ones to increase the likelihood of success in achieving project objectives [17].

2.2 Related research

Judging by the results obtained from a systematic literature review presented in [81] and a search for related research papers about RM ontologies in different application domains (e.g., software engineering, projects and information systems), it is evident that there is a strong interest from researchers and practitioners in helping to present the knowledge and terminology associated with RM practices. Table 2 presents a summary of the relevant characteristics of the related papers concerning: (C1) general purpose of the ontology, (C2) application domain, (C3) method/methodology used in the construction of the ontology, (C4) modelling language applied for the ontological representation, (C5) language for the development of the ontology, (C6) software used in its implementation, and (C7) conceptual support (standards, models, methodologies, etc.) for the design of the proposal.

Table 2 Main characteristics of the related papers

#	Authors	C1	C3	C4	C5	C6	C7
C2: General							
1	Brownsword [12]	To simplify the terminology associated with the RM process and to improve its understanding by the different stakeholders in any type of organisation.	-	UML	-	-	AS/NZS 4360:2004 [4] ISO Guide 73:2007 [58]
2	Ansaldi et al. [3]	A domain ontology to formalise the knowledge associated with RM is proposed through the analysis of ISO standards. This ontology serves as a knowledge base for the development of a tool that supports the choice of the most appropriate risk assessment techniques according to the needs and characteristics of the organisation. A preliminary evaluation of the	Noy and McGuinness [92]	-	-	Protégé	ISO 31000:2009 [59] ISO 31010:2009 [70] ISO Guide 73:2009 [72]

		proposal to check its utility was carried out, assisted by experts. The results of this evaluation and the use of a formal method for the assessment of the proposal are not evidenced.					
3	Sales et al. [117]	To show the relationship between the concepts of value and risk, through the construction of a common ontology which focuses on the process of risk assessment. This relationship is based on experience, i.e., on the way in which risks are judged through the breakdown of smaller events. The purpose is to clarify the internal structure of the risk and its degree of impact on objectives. These judgments are considered by the authors as experience value ascription and experience risk assessment, which involve a value and a risk experience.	-	OntoUML	-	-	Guarino et al. [44] Sales et al. [118]
C2: Educational							
4	Robin and Uma [111]	To identify and organise, from an educational perspective, the concepts and their interrelationships involved in software risk analysis. The authors claim that the ontology can be used as a knowledge base of an information system or as a knowledge repository of an e-learning application on this subject.	-	-	OWL	Protégé	-
C2: Projects							
5	Falbo et al. [27]	A knowledge management approach to support organisational learning about risk management is presented. A software risk ontology is developed, which serves as a knowledge management base for the GeRis developed by the same authors. The evaluation of the ontology is not addressed as part of the scope of this paper.	Falbo et al. [29]	UML	-	-	-
6	Nota et al. [91]	A metamodel for RM in distributed environments is described, whose makes use of a risk ontology based on the SEI guidelines. A set of rules expressed in a logic programming language called RSF is proposed to qualify the operational aspects of RM in distributed environments. The proposal was validated by means of two case studies where the instances of the model applied to a distributed software project carried out by a virtual company and in an environmental project conducted in the Italian region of Campania are presented.	-	-	-	-	CMU/SEI-96-TR-012 [16]
7	Rojrattanakorn et al. [113]	The identification of risks in software projects is tackled by using a knowledgeable ontology. The proposal adopts the risk taxonomy of the SEI and the project planning process area of the CMMI. In addition, it serves as a knowledge base to help reduce workload and subjective risk judgement. It was evaluated through a case study, applied to a software project. Furthermore, a set of questions was defined in SPARQL to help identifying risks in a project concerning the missing work products within the selected process area.	-	-	OWL	Protégé	Risk taxonomy [14] CMMI DEV v 1.3 [120] Soydan and Kokar [123]
8	Yamami et al. [135]	To integrate the knowledge involved in project management in areas such as: scope, schedule, cost, risk and quality. Each of these knowledge areas has its own ontological representation and together form a global ontology for the governance of IT projects. For the evaluation of the ontology, the authors claim to have used the criteria of inconsistency, incompleteness and redundancy. The integrity of the ontology was validated using inference engines Fact ++ 1.6.5 and Pellet. The use of a specific evaluation method was not evidenced.	-	-	OWL	Protégé	PMBOK – 5th Ed [103]
9	Gaspoz et al. [36]	To help prevent risks in projects, the ontology was integrated into an Enterprise Resource Planning (ERP) system to help identify, define and monitor the multiple variables that could impact projects. A verification of the technical accuracy of the ontology through its implementation in Protégé was carried out. The validation of the ontology was performed through its integration into the ERP. A specific evaluation method, as suggested in METHONTOLOGY, was not evidenced.	METHONTOLOGY [32]	-	OWL	Protégé	Literature review
10	Abioye et al. [24]	A software risk ontology (SRO) oriented towards the conceptualisation of project risks is proposed along with a hierarchical risk breakdown structure (HBRS) which aims to support RM tasks. In addition, a technological prototype based on ORS is presented which aims to improve project delivery and reduce the impact of risks. Finally, this proposal was validated using structured questions, expert interviews and case studies.	Boyce and Pahl. [11] Natalya and McGuinness [92]	-	OWL and RDF	Protégé	Literature review, organisational documents, expert interview
C2: Business Processes							

11	Lykourentzou et al. [78]	It is aimed to promote collaboration between the different business areas in the context of operational RM. The proposed ontology supports decision-making and the definition of governance strategies based on the risks identified. As regards the evaluation, a validation of the content and capacity of the ontology was carried out through surveys completed by IT experts from industry and academia.	Ontology Ontogeny [89]	Conceptual network	-	-	ISO 31000:2009 [59] AS/NZS 4360:2004 [4] IRM 2002 [51] ENISA [25]
12	Pittl et al. [101]	An ontology based on a risk catalogue of the German Federal Office for Information Security (IT-Grundschutz) is reviewed. The ontology serves as a knowledge base for the generic classification of risks that can arise in different business processes. It is also part of a tool that, by means of rules and semantic annotations, enables the automatic generation of risk reports.	-	-	OWL	SeMFIS platform	Fill [34] IT-Grundschutz-Katalog [13]
C2: Information technology (IT)							
13	Ahmed et al. [2]	An ontology-based approach to risk assessment is presented. The proposal is oriented to deal with information security problems at the organisational level and was used with the SemanticLIFE framework.	-	-	OWL	-	-
14	Peng and Nunes [45,46]	A theoretical ontology that aims to help identify risks in the post-implementation of the ERP system in an organization is proposed. The ontology is divided into hierarchical levels/categories of risks. The authors validated the suitability of the ontology through surveys sent to operations and IT managers from public sector companies in China.	-	-	-	-	Critical literature review
15	Nurse and Sinclair [93]	A high-level ontology is proposed, which contains the most relevant factors of the RM process that can influence the security requirements of web services and applications in an organisation. The proposal aims to provide a shared conceptualisation of security risks and requirements, which can be used as a knowledge base for a future requirements comparison tool.	King and Reinold [75]	UML	-	-	Existing Security and Risk Ontologies
16	Agrawal [1]	An ontology for the domain of the management of security risks is proposed, which aims to structure and organise the basic concepts of the risk assessment phase in information security, according to the guidelines proposed by the ISO 27005 standard. The proposal was validated through a case scenario, where instances of the ontology were created to verify its potential use in a health clinic.	Noy and McGuinness [92]	-	OWL	protégé	ISO 27005:2011 [60] ISO 27000:2014 [62]

Acronyms and Abbreviations - C1: General purpose of the ontology, C2: Application domain, C3: Method/Methodology, C4: Modelling language, C5: Ontology language, C6: Implementation software, C7: Conceptual Support

Based on the analysis of the related research results, some important aspects of the ontologies and their limitations are presented below:

(i) It is possible to observe that the trends of the cited papers on RM ontologies have been focused on the following application domains:

- General level, to simplify and improve the understanding of this topic [12]; to disseminate the relationship between the concepts of value and risk on the basis of experience along with its contribution to risk assessment [117]; and to support the selection of techniques for risk assessment according to the characteristics and needs of an organisation [3].
- Educational level, to assist in training on software risk analysis [111].
- Project level, to help integrate RM into IT project governance practices [135]; to assist with RM in distributed software projects and to qualify the operational aspects of their realisation [91]; to support RM and assist in risk prevention through its integration into an ERP system [36]; to support automated risk identification in software projects [113]; to support RM learning in organisations and serve as a knowledge base for decision-making about risks of software processes and projects [27] and to undertake risk classification based on the software life cycle, through the use of an HBRS and assist in qualitative risk analysis using analytical hierarchical process (AHP) [24].

- Business process level, to identify and classify process risks and the automatic generation of risk reports [101]; to promote the collaboration and communication in operational RM of the different business areas and to support decision-making [78].
- IT level, to help identify risks that arise after the implementation of ERP systems [45,46]; to structure and organise the concepts related to information security risk assessment [1]; to support the assessment of risks related with information security aspects at the organisational level, based on the attacks and vulnerabilities that information systems may suffer [2]; and to have a shared conceptualisation of security risks and requirements in web services and applications [93].

(ii) In the analysis of related literature, it can be seen that it is necessary to be more rigorous in the development of ontologies due to the fact that very few studies report the method chosen for their development, which can limit the scientific rigor, coherence and quality. Furthermore, most of the ontologies have not been represented using a modelling language; they are described using natural language at a very high level and with very little detail, which in some cases makes it difficult to grasp and/or understand the relationships between the concepts and the knowledge they represent. Similarly, very few proposals evidence the use of a formal language for ontology construction (e.g., OWL, RDF, etc.) and the use of software tools for implementation and editing. In the case of the articles in which the authors stated that they had implemented the ontology, none of them shared a website or web repository to access the resources. As a result, it is not possible to do a better analysis and reuse of the formalised knowledge.

(iii) In several ontologies, the absence of definitions of domain concepts and their relationships was noted, which generates confusion in interpretations and therefore does not contribute to improving the body of knowledge of RM. Hence, it is necessary to support the creation of a consistent terminology to improve the understanding, application and reuse of knowledge associated with RM. However, in [1,12,78,93] the authors included the definition of some relevant concepts of the RM domain, in order to ensure that its scope could be understood. However, these are proposals that are based on standards that have already been withdrawn or replaced by the institutions that manage them.

(iv) The ontologies have different purposes and abstraction levels. Furthermore, they have a high degree of heterogeneity in the terminology used to represent the RM domain, which makes it difficult to understand what the essential elements should be in carrying out this management practice. This is also due to the fact that researchers only focus on a very high-level description of RM activities/phases/steps and/or use scenarios.

(v) It was also noted that RM is considered in different proposals at an operational level and from a traditional approach, which evidence the need to develop ontologies to formalise the establishment and control of a RM strategy at any level of the organisation, which provide the key elements to support the definition of the RM context and the risk criteria or parameters necessary to support decision-making during RM. It is also required to support this practice throughout the life cycle of an organisation's asset and to contribute to the proper management of the risk profile of the assets. These new initiatives should also help to cover the RM domain in the context of the software life cycle and be supported by international standards/models/frameworks that are widely recognised by the industry. This is in order to help significantly reduce the ambiguity of terminology associated with this management practice.

In short, the studies analysed and discussed above provide valuable information on RM at a high level and in different application domains. These are specifically focused on supporting this management practice at the operational level, leaving aside other levels of organisational management, which are a fundamental part of having a

holistic view of risk that helps to preserve organisational value through RM practices. Some ontologies lack of formal methods for their development and/or the use of modelling languages that allow their representation and implementation through computer tools. These results, added to those achieved in [66], show the need to help formalise and improve the process of RM, through the definition of proposals that significantly reduce the ambiguity, inconsistencies and incompleteness in the terminology, concepts and definitions associated with this domain. In this sense, a first step is to establish a formal description of the knowledge related to software risk management that helps to integrate, understand and organise the concepts, terms and their relationships around different process structures defined in approaches and frameworks widely recognised by the industry. It is important to note that this step is part of a broader research, which has as its main objective "*to define a methodological framework for risk management that will provide an organisation with a framework for establishing an integrated approach to RMS, which allows for a holistic view of risk and helps to guide RM practices and preserve its value at any level of the organisation. Furthermore, the methodological framework will establish a framework that will facilitate the different stakeholders to carry out an adequate risk management of their assets and increase the effectiveness and performance of this practice in the organisation*".

Therefore, the general question that guided this research was:

Is it possible to create an ontology that allows grouping the fundamental concepts and relationships to describe risk management knowledge at any level of the organisation?

In order to provide an answer to this question, this paper presents an ontology that aims to formalise the terminology associated with the RM process at different levels of the organisation, in order to provide a unified view through a common language that helps to reduce ambiguities and allows researchers and practitioners in the software industry to have a better understanding of this topic and lay the foundations for further research to improve and automate RM practices.

3 ONTOLOGIES AND THEIR REPRESENTATION FORMALISM

An ontology is an abstract and explicit representation of the elements (objects, concepts, entities, and their relationships) belonging to a domain of knowledge or area of interest that is common and shared [41]. Ontologies are used to formalise or determine the knowledge of a specific domain [124] in a formal and generic way so that it can be shared through applications and groups of people [40]. Therefore, an ontology is an explicit knowledge-level specification of a conceptualisation [48]. As such, ontologies help to solve problems of integrity and consistency in the terminology used in a given context, by means of a common vocabulary or terminology that helps to minimise ambiguities [19,28,30,35,128], and which is possible by means of knowledge integration [30,49,116].

There are different types of ontologies, such as high-level ontologies, domain ontologies, application ontologies and information ontologies [19,31,43,114,124]. Domain ontologies, which is the type of ontology presented in this paper, allow one to express conceptualisations of a specific context [124] through the capture of knowledge [31], the definition of concepts and their relationships with respect to the activities that take place in the domain, and the theories and principles that govern them [40].

On the other hand, although different methods and methodologies exist to support the elaboration of ontologies - such as those analysed in [40] the Cyc method, Uschold and King's method, Grüninger and Fox's methodology, the KACTUS method, METHONTOLOGY, the SENSUS method, and the On-To-Knowledge methodology - it was decided to use the "representation formalism for software engineering ontologies" (REFSENO) [126], which is an enhanced adaptation of METHONTOLOGY [19]. REFSENO, proposed by the Fraunhofer Institute for Experimental Software

Engineering (IESE), makes possible [126]: (i) knowledge modelling in a precise and consistent way, in this case with graphic representation using concept diagrams, which are similar to the class diagrams in UML; (ii) the definition of an ontology in a clear and precise way through the identification and detailed definition of the concepts and their main relationships, by means of a set of tables; and (iii) the validation of the ontology to check its consistency and suitability, which can be done through instances or case studies. Other methodologies only allow less intuitive and complex representations and are intended for people who are not familiar with first-order predicate logic or similar.

3.1 Brief description of the methodology and its use

The methodology followed for the development of the ontology was REFSENO [126], which establishes four main stages:

- **Stage 1**: The main sources of knowledge to be used in the development of the ontology were established, which are listed in Table 3 and were analysed in section 2.1.
- **Stage 2**: The purpose, main objective of the ontology and the usage scenarios regarding the application of RM at the different management levels of the organisation were stated. These scenarios allowed determining the scope of the ontology and structuring the knowledge to produce the subontologies. To help determine the scope, a set of competency questions (CQs) were established through natural language [40]. These CQs are also intended to help verify the concepts and their relationships, and to determine whether they are necessary and sufficient to cover the domain, once the ontology is implemented. Additionally, all the main concepts related to the usage scenarios were identified by conducting an analysis of each of the main sources described in Table 3.
- **Stage 3**: The ontology was conceptualised and represented through different iterations. The terminology identified in stage 2 was compared, similarities were looked for and where necessary harmonised to eliminate ambiguities and propose a common terminology. For the definition of the terms, a source was used to provide an explicit definition of the term or several definitions were adapted as necessary to achieve consistency with respect to the domain represented by the ontology. In the case that the main sources did not present a glossary of terms and definitions, the family of standards or products related to these main sources was used to define the concepts. Also, the semantic relationships between the different concepts and their representation were identified and defined using the UML notation. By carrying out the relationship of the concepts, commonalities between two or more concepts were analysed and as a result, if it was necessary, they were included in the glossary (these were the concepts introduced for modelling purposes). Finally, an instance of the ontology was created to carry out a conceptual validation.
- **Stage 4**: The operational implementation of the ontology was carried out through the Protégé tool, to verify the knowledge representation through the CQs.

The results of each of these steps are described in more detail in the following section.

Table 3. Sources of knowledge utilised to construct the ontology

Key		Source Name	Reference
D1		Main documents for ontology definition	
	D1a	Risk Management – Guidelines	ISO 31000:2018 [71]
	D1b	COBIT 2019 Framework: Introduction and Methodology	COBIT 2019 Framework [55]
	D1c	A Guide to the Project Management Body of Knowledge	PMBOK 6th ed. [104]
	D1d	Capability Maturity Model Integration Version 2.0	CMMI V2.0 [17]
D2		Other standards/frameworks/models/techniques/studies related to RM	
	D2a	Systems and software engineering — Life cycle processes — Risk management	16085:2021 [68]
	D2b	Risk management — Vocabulary	ISO Guide 73:2009 [72]
	D2c	COBIT 5 for Risk	COBIT 5 for Risk [52]
	D2d	Practice Standard for Project Risk Management	PMI [102]
	D2e	Taxonomy-Based Risk Identification	CMU/SEI-93-TR-006 [14]
	D2f	Risk factors in software development projects: a systematic literature review	Menezes et al. [83]
D3		Documents related to software processes, projects, enterprise governance of IT, information security, asset management, etc.	
	D3a	Systems and software engineering -- Software life cycle processes	ISO 12207:2017 [69]
	D3b	Capability Maturity Model Integration for Development Version 1.3	CMMI-DEV Version 1.3 [120]
	D3c	Software & Systems Process Engineering Meta-Model Specification V2.0	SPEM V2.0 [96]
	D3d	Managing Successful Projects with PRINCE2	PRINCE2 6th ed. [5]
	D3e	COBIT 5: A Business Framework for the Governance and Management of Enterprise IT	COBIT 5 Framework [53]
	D3f	COBIT 5 Enabling Processes	COBIT 5 Enabling Processes [54]
	D3g	Information security management	ISO 27001:2013 [61]
	D3h	Asset management - Overview, principles and terminology	ISO 55000:2014 [63]
	D3i	Systems and software engineering — Measurement process	ISO 15939:2017 [66]
D4		Ontologies related with GR	
	D4a	Ontology-based operational risk management	Lykourentzou et al. [78]
	D4b	Learning How to Manage Risks Using Organisational Knowledge	Falbo et al. [27]
D5		Ontologies in the software engineering field	
	D5a	Software process ontology	Falbo et al. [28]
	D5b	Ontology of Process-reference Models	Pardo et al. [98]
	D5c	Ontology for Software Development Governance	Masso and Pardo [80]
	D5d	e-Government project management ontology	Sarantis et al. [119]
D6		General definitions	
	D6a	A Paradigmatic Analysis Contrasting Information Systems Development Approaches and Methodologies	Livari et al. [50]

4 SOFTWARE RISK MANAGEMENT ONTOLOGY

Considering the above analysis of the current situation, it is important to help reduce ambiguity in the terminology related to RM. To this end, this section presents the development of a domain ontology for software RM from an integrated approach. The ontology is obtained through the analysis, comparison and integration of different solutions for RM, and for its definition we pursued the following goals which were adapted from [10,35,99]:

- Locate and identification of terms, synonyms and homonyms, inconsistencies, and terminological conflicts.
- Integration of the concepts found in the reference literature.

These objectives can be achieved through a common ontology that represents the domain for RM. The proposed ontology should define all concepts, providing terms with clear and concise definitions which precisely identify the relationships between them. Also, an ontology in this research domain can serve as the basis to support RM in an organisation, its main objective being to define and establish an RMS that supports the different organisational levels in an integral way and makes possible the measurement and control of RM activities. It also defines the different risk criteria that will support the decision-making needed to manage the risk profiles of the different processes and projects carried out in an organisation.

Bearing this in mind, we set out in the following section the software risk management ontology (SRMO).

4.1 SRMO: Software Risk Management Ontology

SRMO is a domain ontology which was designed using some of the most widespread, industry-recognised RM solutions, including: ISO 31000:2018, CMMI V2.0, PMBOK and COBIT 2019. Additionally, the ISO 16085:2021 [68] standard was considered, which is oriented to RM in the life cycle of Systems and Software Engineering projects. Furthermore, this standard facilitates the application of the ISO 31000:2018 standard in this context. ISO 16085 has

been designed to be applied to systems and software life cycle processes through the standards ISO 15288:2015 [64], ISO 12207:2017 [69], and ISO 9001:2015 [65], among others.

SRMO seeks as its principal objective to establish a common terminology that allows organisations and professionals engaged in software development to understand which are the key and fundamental elements in carrying out an RM in the context of the software life cycle, with emphasis on processes and projects. By using the REFSENO methodology, the represented knowledge with SRMO has been organised into three domain subontologies, which, when integrated, provide a more complete and clearer view of each of the concepts related to RM (see Figure 1).

As can be observed in Figure 1, the subontology for the establishment of risk management (RMEO) lies at the core of this proposal, since its concepts are used by the other subontologies. RMEO aims to provide an organisation with each of the elements that it needs to establish the RM process from an integrated perspective. The Risk Context Establishment subontology (RCEO) presents each one of the elements (e.g., risk categories, risk types, risk thresholds, etc.) needed to help identify, analyse and evaluate the risks in an organisation. Finally, the Risk Profile Management subontology (RPMO) is intended to provide the necessary components to support the management of the risks which can affect an organisation asset. Therefore, SRMO is the integration of each of the concepts and relationships represented in these subontologies.

The description of the SRMO ontology and its subontologies in terms of its purpose, the glossary of concepts and their relations, along with their graphic representation by using UML, are shown in the following subsections. Due to space limitations, the description of the attributes associated to each of the concepts was omitted.

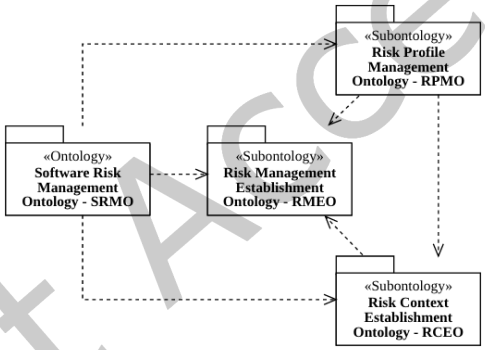

Figure 1: Software risk management ontology and relationships between its subontologies.

4.1.1 Risk Management Establishment Ontology (RMEO).

4.1.1.1 Purpose.

The RMEO subontology provides a conceptual framework that identifies the basic elements that must be considered by an organisation in carrying out the design and establishment of an RMS from an integrated approach (see Figure 2). It also provides a holistic view of RM, which can be implemented at any level of the organisation, in which the processes and projects (*with all their constituent elements*) are considered as key assets of the organisation. These assets are worth protecting since any damage to them could impact negatively on the business and its ability to fulfil its aims and objectives. The purpose of RMEO is to establish an RM that is adapted to the needs of the business and that helps to: (i) Meet the objectives of the business strategy and of each of its assets through the systematic application of RM practices; (ii) Promote a risk culture that helps to maintain the value of the organisation; (iii) Establish a consistent

approach for the RM which is in line with the size and nature of the organisation and which clearly describes the RM process, including the management practices (i.e., activities, tasks and steps) and resources necessary to conduct the RM (in the case of the roles and/or organisational structures, the level of responsibility assigned for RM practices should be specified); and (iv) Monitor, measure, and evaluate RM practices and strategy through the establishment of control points for the improvement of the RM processes and capabilities of the organisation, in order to make them sustainable over time. Finally, this subontology should be able to respond to the following competency questions (CQs):

- CQ1: What are the established objectives and metrics for an RMS?
- CQ2: What are the RM process tasks associated with an RMS, what are the management resources allocated to them, and what is their accountability?
- CQ3: What are the objectives and metrics assigned to an RM process?
- CQ4: What are the procedures that can be used in the tasks of an RM process?
- CQ5: What are the active strategies for managing risks, what scope do they have, and through which approach are they implemented?

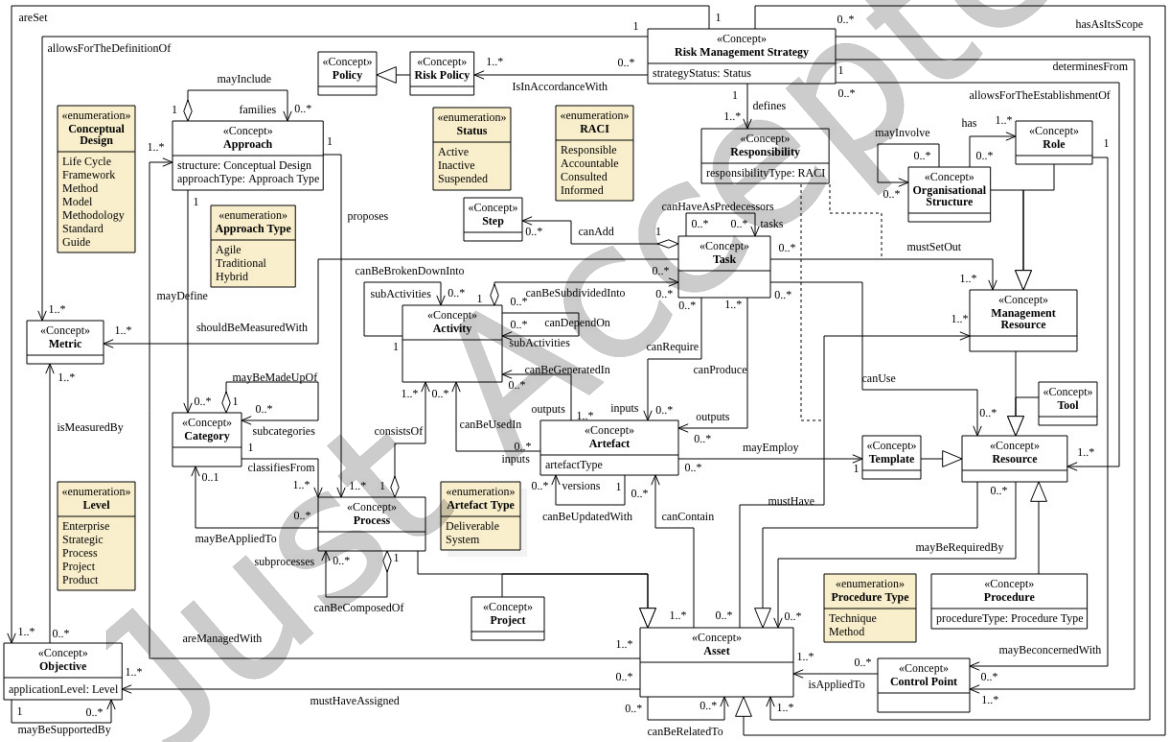

Figure 2: UML representation of Risk Management Establishment Ontology (RMEO).

4.1.1.2 Concepts and relationships of RMEO.

The precise definitions of the RMEO concepts are presented (alphabetically ordered) in Table 4 as follows: the first column shows the term, the second column shows the related super concept, the third includes the definition of the term, and the fourth shows the source of the term (and where it has been cited, adopted, or adapted). Table 5 shows

the relationships between the concepts shown in Table 4. The descriptions shown in the fourth column of Table 4 use the following nomenclature: Cited in [source], if the term has been cited by a source and this is not the main source (in this case the term has not been modified); Taken from [source], if the term has been defined in another source but it is necessary for this this ontology and therefore has not been changed or adapted; Adapted from [source], if the term has been defined in one or several sources and some changes or adjustments have been made to complement or adapt the term to the context of the ontology. This same structure has been used for all the subontologies.

Table 4: Definition of the terms in the RMEO

Term	Super-concept	Definition	Source
Activity	Concept	An activity is a set of tasks or actions to be performed and which describes how to achieve the objectives of the process. To be accomplished, an activity requires or adopts different types of resources (procedures, roles, tools, etc) and may depend on other activities or divide into sub-activities to achieve the same objective. Additionally, during its accomplishment an activity may create and modify artefacts (work products).	Adapted from: Falbo et al. [28], Pardo et al. [98]
Approach	Concept	An approach is a conceptual structure that describes and formalises a set of good practices belonging to a specific domain. It consists of a set of fundamental concepts, objectives, rules, or guidelines, which are organised in a structured way. An approach may be used by one or more types of organisations.	Adapted from: Livari et al. [50]
Artefact	Concept	An artefact (product or work product) is any kind of element capable of being created, used, or updated during the life cycle of an asset. Artefacts are frequently the results of carrying out a task, whether these be independent or part of a solution. They may also be regarded as necessary to support the execution of an asset. Artefacts can be input or output, mandatory or optional, and used in one or many assets. Two kinds of artefacts are generally recognised: deliverables and systems. The granularity of the results of an artefact will be determined by the nature of the asset (e.g., lessons learned (deliverable), a module of a software system (system), risk management plan (deliverable), etc.).	Adapted from: CMMI V2.0 [17], Falbo et al. [28], Pardo et al. [98], Sarantis et al. [119]
Asset	Concept	An asset is any item, thing or entity that has a tangible or intangible value, whether financial or not, for an organisation and its stakeholders. Assets contribute to obtaining the goals and objectives of an organisation and, as such, are worth protecting, as if they are damaged, they could impact negatively on the business.	Adapted from: CMMI-DEV Version 1.3 [120], ISO 55000:2014 [63], COBIT 5 for Risk [52]
Category	Concept	Categories are logical groups of related processes that address common problems encountered by any type of organisation.	Adapted from: CMMI V2.0 [17]
Control point	Concept	Set of specific actions that facilitate control of the processes defined in an organisation through the permanent monitoring of the process, the evaluation and measurement of the execution of the process, and the recommendation of corrective and preventive actions that improve the process.	Adapted from: ISO 31000:2018 [71], PMBOK 6th ed. [104]
Management resource	Resource	These are all the organisational structures and roles required by an organisation to carry out the activities of governance and management of its business processes.	Adapted from: COBIT 5 for Risk [52]
Metric	Concept	A metric is a quantifiable entity that enables the measurement of the degree of achievement of an objective of any asset of the organisation. A metric can be used to anticipate the appearance of a risk, as well as to support the monitoring and control of risks. In these cases, it is called a "trigger".	Adapted from: COBIT 5 Framework [53], COBIT 5 for Risk [52]
Objective	Concept	Something toward which work is to be directed, a strategic position to be attained, a purpose to be achieved, a result to be obtained, a product to be produced, or a service to be performed.	Taken from: PMBOK 6th ed. [104]
Organisational structure	Management resource	It is an entity (committee, business unit, etc.) that helps with the governance and management tasks of the organisation. These entities have associated functions and responsibilities. In addition, they are responsible for making decisions in the different business processes, allowing management to be carried out effectively and efficiently.	Adapted from: COBIT 2019 Framework [55], COBIT 5 for Risk [52]
Policy	Concept	It describes the basic principles formally expressed by the managers of an organisation, which are intended to influence and guide decision-making, so that decisions are aligned with the objectives and strategies defined by the organisation.	Adapted from: CMMI-DEV Version 1.3 [120], COBIT 5 for Risk [52], PMBOK 6th ed. [104], Masso and Pardo [80]
Procedure	Resource	It is any method or technique adopted by the organisation to achieve consistent performance or results when the main activities of the business are being carried out. For example, the methods systematically define the step-by-step of how a process activity should be carried out. A technique, meanwhile, is a less rigorous procedure than a method. That is, it has a practical approach to the implementation of a specific process activity.	Adapted from: Falbo et al. [28]
Process	Asset	Generally, this is a collection of practices influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs, and produces outputs (e.g., products, services)	Taken from: COBIT 5 Framework [53]
Project	Asset	A temporary endeavour undertaken to create a unique product, service, or result.	Taken from: PMBOK 6th ed. [104]
Resource	Asset	Any asset of a company that can be used or consumed during the execution of a process and that can help the organisation to achieve its objectives.	Adapted from: ISO 12207:2017 [69], COBIT 5 Framework [53]
Responsibility	Concept	It represents the different types or levels of responsibilities that can be undertaken by the management resources involved in an RMS. The responsibilities are the obligations for or the authorities over each of the resources in the tasks and processes related with the assets involved in the scope of an RMS. Responsibilities can be associated with those defined in the RACI matrix (Responsible, Accountable, Consulted, Informed) and an organisation can make use of a responsibility assignment matrix (RAM) to carry out their allocation.	Adapted from: PMBOK 6th ed. [104], COBIT 5 Framework [53], COBIT 5 Enabling Processes [54]
Risk management	Asset	A set of elements that guide the activities of RM at any level of an organisation (strategic,	Adapted from:

strategy		project, software life cycle, among others). A risk management strategy (RMS) aims to help an organisation increase the probability of achieving its objectives and to reduce the impact of risks at any level, providing the necessary elements to support decision-making, in order to counteract risks. It also enables the establishment of control mechanisms to monitor, measure and evaluate the RM process of the organisation, with the aim of continuously improving it within the organisation.	CMMI-DEV Version 1.3 [120], CMMI V2.0 [17], ISO 31000:2018 [71]
Risk Policy	Policy	It is a specific policy that allows the risk management process to be formalised through a basic set of principles that should govern the organisation's actions in conducting RM process activities.	Adapted from: PMBOK 6th ed. [104]
Role	Management resource	Describes a set or group of responsibilities, duties and skills required to perform a specific activity.	Cited in: Pardo et al. [98]
Step	Concept	Describes a specific and coherent part of the work to be carried out in a task. A group of steps represents all the work that must be undertaken to achieve the overall objective of a task. Not all steps are mandatory to carry out a task in a process.	Adapted from: SPEM V2.0 [96]
Task	Concept	Process element that defines the work done by roles. A task is associated with the input and the output products.	Taken from: Pardo et al. [98]
Template	Resource	A partially complete document in a predefined format that provides a defined structure for collecting, organising and presenting information and data.	Taken from: PMBOK 6th ed. [104]
Tool	Resource	A software program, which may have a general or a specific purpose, which allows for automatically carrying out a given activity with the aim of producing a product or result.	Adapted from: PMBOK 6th ed. [104], Pardo et al. [98]

Table 5 presents the relationships between the RMEO concepts:

Table 5: Relationships in the RMEO

Name	Concepts	Description
Allows for the definition of	Risk management strategy – Metric	A risk management strategy allows for the definition of one-to-many metrics. A metric is defined by a risk management strategy.
Allows for the establishment of	Risk management strategy – Resource	A risk management strategy allows for the establishment of one-to-many resources. One resource can be used in many risk management strategies.
Are managed with	Asset – Approach	All the assets are managed with one or more approaches. An approach can be used to manage one to many approaches.
Are set	Risk management strategy – Objective	In a risk management strategy, one to many objectives are set. An objective is defined by a risk management strategy.
Can add	Task - Step	A task can add many steps. Many steps are used in a task.
Can be broken down into	Activity - Activity	An activity can be broken down into many other activities (subactivities).
Can be composed of	Process – Process	A process can be composed of many other processes (subprocesses).
Can be generated in	Artefact - Activity	An artefact can be generated in one or many activities. An activity has as output one or many artefacts.
Can be related to	Asset – Asset	An asset can be related to other assets. An asset can be required by other assets.
Can be subdivided into	Activity - Task	An activity can subdivided into many tasks. A task is part of an activity.
Can be updated with	Artefact - Artefact	An artefact can be updated with many other artefacts (versions).
Can be used in	Artefact - Activity	An artefact can be used in one or many activities. An activity has as input one or many artefacts.
Can contain	Asset - Artefact	An asset can contain many artefacts. An artefact can be used in many assets.
Can depend on	Activity - Activity	An activity can depend on other activities. An activity can interact with other activities.
Can have as predecessors	Task - Task	A task can have as predecessors many other tasks (subtasks).
Can produce	Task - Artefact	A task can produce many artefacts as outputs. An artefact can be output of one or many tasks.
Can require	Task - Artefact	A task can require many artefacts as inputs. An artefact can be input of one or many tasks.
Can use	Task – Resource	A task can use many resources. One resource can be used by many tasks.
Classifies from	Category – Process	A category classifies from one-to-many processes. A process is categorised by a category.
Consists of	Process – Activity	A process consists of one-to-many activities. An activity is part of a process.
Defines	Risk management strategy - Responsibility	A risk management strategy defines one to many responsibilities. A responsibility is defined in a risk management strategy.
Determines from	Risk management strategy – Control point	A risk management strategy determines from one-to-many control points. A control point is established by a risk management strategy.
Has	Organisational structure – Role	Each organisational structure has one or many roles. A role can be involved in one or many organisational structures.
Has as its scope	Risk management strategy – Asset	Each risk management strategy has as its scope one or many assets. An asset can be involved in many risk management strategies.
Is applied to	Control point – Asset	A control point is applied to one or more assets. An asset may or may not have many checkpoints applied to it.
Is in accordance with	Risk management strategy – Risk policy	A risk management strategy is in accordance with one or many risk policies. A risk policy can be considered by many risk management strategies.
Is measured by	Objective – Metric	An objective is measured by one or many metrics. One metric allows many objectives to be measured.
May be applied to	Process – Category	A process may or may not be applied to a category. And many processes can be applied to a category.
May be concerned with	Role – Control point	One role may be concerned with many control points. A control point is governed by a role.
May be made up of	Category – Category	A category may or may not be made up of many categories (subcategories).
May be required by	Resource - Asset	A resource may be required by one or many assets. One asset may require many resources.
May be supported by	Objective – Objective	An objective may or may not be supported by other objectives.
May define	Approach – Category	An approach may or may not define many categories. A category is defined by an approach.
May employ	Artefact - Template	An artefact may employ a template. A template can be used for creating many artefacts.
May include	Approach – Approach	An approach may or may not include other approaches (families).
May involve	Organisational structure – Organisational structure	An organisational structure may involve many other organisational structures. An organisational structure may be involved with many other organisational structures.
Must have	Asset - Management resource	Each asset must have one or many management resources. A management resource can be assigned to one or many assets.

Must have assigned	Asset – Objective	Each asset must have assigned one or many objectives. An objective can be assigned to one or many assets.
Must set out	Task - Management resource	A task must set out one or many management resources. A management resource can be responsible for many tasks.
Proposes	Approach – Process	An approach proposes one to many processes. A process is defined by an approach.
Should be measured with	Task - Metric	A task should be measured with one or many metrics. One metric allows many tasks to be measured.

4.1.2 Risk Context Establishment Ontology (RCEO).

4.1.2.1 Purpose.

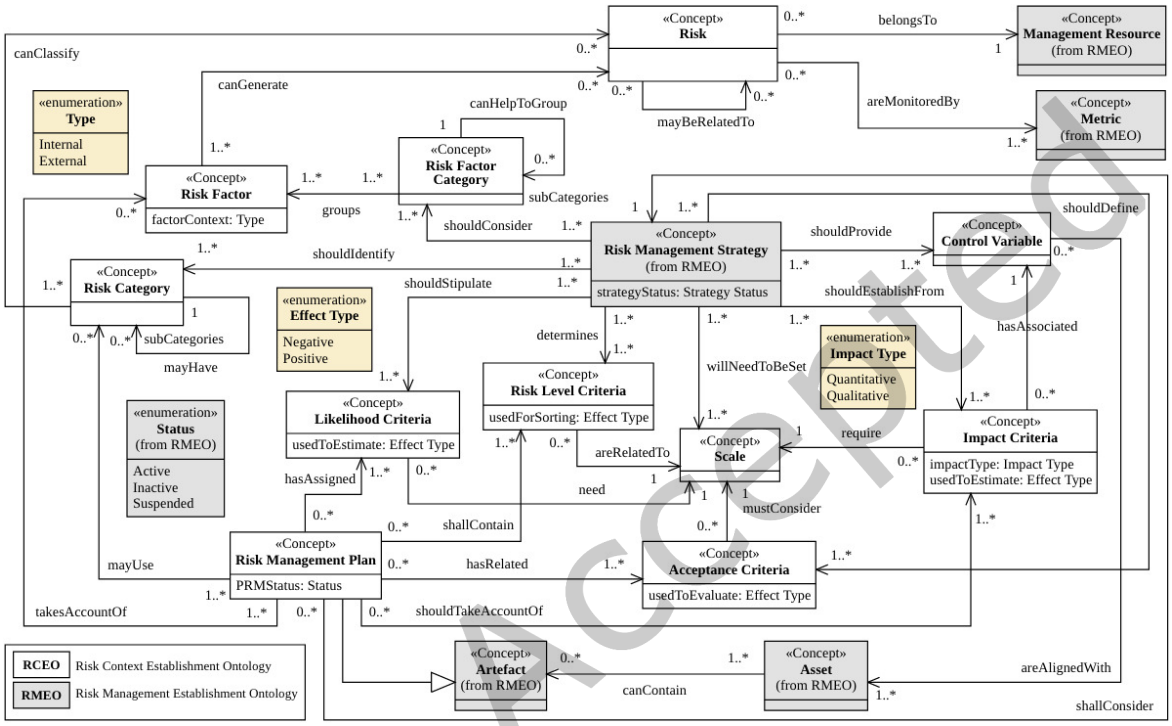

Figure 3: UML representation of Risk Context Establishment Ontology (RCEO).

This subontology provides the basic mechanisms for an organisation to define and establish the risk criteria or parameters that are required to carry out the RM (see Figure 3). It also identifies the different sources of risk that will allow the classification of the risks to which the different assets of the organisation are exposed, together with their different triggering factors. The RCEO allows one to establish the different levels of risk acceptance and tolerance that an organisation is prepared to assume to fulfil its objectives. The risk criteria should be aligned with the scope of the strategy and the approach selected for the RM and should be documented in the risk management plan of an asset. These criteria are also the reference parameters on which the importance of a risk can be determined, depending on its probability and impact on the asset objectives. Therefore, these criteria should be consistent as they will support the risk assessment process to estimate, evaluate, classify and prioritise risks throughout the process. Consequently, the RCEO subontology should address the following CQs:

- CQ6: What are the identified risk categories and subcategories in an RMS?
- CQ7: Which assets of the organisation are implementing an RMS?

- CQ8: What are the acceptance criteria defined in an RMS and which are considered by an asset of the organisation?
- CQ9: What risk factors are taken into account by an asset of the organisation and what risks do they cause?
- CQ10: What impact criteria are related to an asset of the organisation and with which control variables are they associated?

4.1.2.2 Concepts and relationships of RCEO.

The precise definitions of the RCEO concepts are presented in Table 6, while in Table 7 the relations between these concepts are shown.

Table 6: Definition of the terms in the RCEO

Term	Super-concept	Definition	Source
Acceptance criteria	Concept	A set of criteria established by an organisation to support risk assessment. Risk acceptance criteria are made up of levels and metrics that will serve as a reference to determine whether the risks are acceptable or require handling. Some of these acceptance levels include: acceptable, tolerable and unacceptable, etc.	Adapted from: ISO 27001:2013 [61]
Control variable	Concept	These are key aspects to be managed when a certain asset of the organisation (e.g., process, product, project) is being carried out. The variables are also known as constraints, i.e., limiting factors that affect the execution of any asset. These variables serve as a support for measuring the impact of the risks. For example, some of the constraints used to measure the impact of risk in projects are: time, cost, quality, among others.	Adapted from: PRINCE2 6th ed. [5]
Impact criteria	Concept	It allows one to measure the positive or negative effects of the occurrence or manifestation of a risk in the organisation. Impact represents the different consequence levels of a risk and can be expressed qualitatively or quantitatively. Additionally, the impact will have associated to it a variable that will enable one to focus on the measurement of the effect of the risk when it occurs.	Adapted from: COBIT 5 for Risk [52], Lykourentzou et al. [78], PMBOK 6th ed. [104]
Likelihood criteria	Concept	This is understood as the possibility of an event occurring. It is a measure to indicate the frequency of occurrence of a risk in a determined period. It can be quantitative or qualitative and can be described using general or mathematical terms.	Adapted from: ISO 31000:2018 [71], COBIT 5 for Risk [52]
Risk	Concept	An uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives.	Taken from: PMBOK 6th ed. [104]
Risk category	Concept	Also known as risk sources or risk types. A category allows for the identification and grouping of risks pertaining to one type of assets of the organisation. In addition, categories can be divided into common groups, adopting a hierarchical structure with the necessary levels to understand the risk exposure of an asset of the organisation. This hierarchical structure is called the Risk Breakdown Structure (RBS)/risk taxonomy, which are methods used to identify and classify risks. These methods can be generic, specific, or tailored to an organisational asset.	Adapted from: PMBOK 6th ed. [104], PMI [102], CMU/SEI-93-TR-006 [14]
Risk factor	Concept	It is a condition that has the potential to cause risks, which can be in the internal or external context of an organisation. Risk factors are causes of risk events/scenarios that can have a positive/negative effect on assets. An internal risk factor can be related to financial, legal, management, planning, etc. aspects, while an external factor can be related, for example, to any component of the PESTEL analysis (Political, Economic, Social, Technological, Environmental, Legal).	Adapted from: ISO 31000:2018 [71], PMBOK 6th ed. [104]
Risk factor category	Concept	It provides a hierarchical structure to carry out the identification and grouping of the different risk factors associated with an asset of the organisation. These categories can be related to the risk categories represented in the RBS/taxonomies used in risk identification and classification.	Adapted from: COBIT 5 for Risk [52], Menezes et al. [83]
Risk level criteria	Concept	These are all the criteria defined by the organisation to classify the risk level of their assets. These levels are determined in accordance with the magnitude of a risk (also called combination of risks, expressed in terms of the combination of impact and their likelihood). The definition of these criteria allows one to evaluate the risks and to take decisions about them.	Adapted from: COBIT 5 for Risk [52], ISO Guide 73:2009 [72]
Risk management Plan	Artefact	It is a component of the strategic plan of the organisation which facilitates the implementation of the risk management strategy as well as defining how the risks of an asset should be managed.	Adapted from: PMBOK 6th ed. [104], ISO 16085:2021 [68]
Scale	Concept	An ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped.	Taken from: ISO 15939:2017 [66]

Table 7: Relationships in the RCEO

Name	Concepts	Description
Are aligned with	Control variable – Asset	All the control variables are aligned with an asset. One asset can have many control variables related to it.
Are monitored by	Risk – Metric	All the risks are monitored by one or many metrics. One metric can monitor many risks.
Are related to	Risk level criteria - Scale	Risk level criteria are related to a scale. One scale may be required by many risk level criteria.
Belongs to	Risk – Management resource	A risk belongs to a management resource. A management resource can own many risks.
Can classify	Risk category – Risk	Each risk category can classify many risks. A risk can be classified into many risk categories.
Can generate	Risk factor – Risk	Each risk factor can generate many risks. A risk is generated by one or many risk factors.
Can help to group	Risk factor category – Risk factor category	A risk factor category can help to group or not many other risk factor categories (subcategories).
Determines	Risk management strategy – Risk level criteria	A risk management strategy determines one or many risk factor categories. Risk level criteria are considered by one or many risk management strategies.
Groups	Risk factor category – Risk factor	Each risk factor category groups one or many risk factors together. A risk factor can be grouped by one or many risk factor categories.
Has assigned	Risk management plan – Likelihood criteria	A risk management plan has one to many likelihood criteria assigned. Likelihood criteria can be assigned to many risk management plans.
Has associated	Impact criteria – Control variable	An impact criterion has a control variable associated with it. One control variable can be associated with many impact criteria.
Has related	Risk management plan – Acceptance criteria	A risk management plan has one to many acceptance criteria related. One acceptance criterion can be related to many risk management plan.
May be related to	Risk – Risk	Each risk may be related to many other risks.
May have	Risk category - Risk category	A risk category may or may not have many other risk categories (subcategories).
May use	Risk management plan – Risk category	A risk management plan may or may not use many risk categories. One risk category is used on many risk management plans.
Must consider	Acceptance criteria – Scale	Acceptance criteria must consider a scale. A scale can be considered by one or many acceptance criteria.
Need	Likelihood criteria – Scale	Likelihood criteria need a scale. A scale can be required for many likelihood criteria.
Require	Impact criteria – Scale	Impact criteria require a scale. One scale may be required by many impact criteria.
Shall Consider	Risk management plan – Risk management strategy	Each risk management plan shall consider a risk management strategy. A risk management strategy is considered by one or many risk management plans.
Shall contain	Risk management plan - Risk level criteria	Each risk management plan shall contain one or more risk level criteria. Risk level criteria can be used in many risk management plans.
Should consider	Risk management strategy – Risk factor category	A risk management strategy should consider one or many risk factor categories. A risk factor category is considered by one or many risk management strategies.
Should define	Risk management strategy – Acceptance criteria	A risk management strategy should define one or many risk acceptance criteria. One risk acceptance criterion is defined by one or many risk management strategies.
Should establish from	Risk management strategy – Impact criteria	A risk management strategy should establish from one-to-many impact criteria. One impact criterion is established by one or many risk management strategies.
Should identify	Risk management strategy – Risk category	A risk management strategy should identify one to many categories of risk. A category of risk is identified by one or many risk management strategies.
Should provide	Risk management strategy – Control variable	A risk management strategy should provide one to many control variables. A control variable is defined by one or many risk management strategies.
Should stipulate	Risk management strategy – Likelihood criteria	A risk management strategy should stipulate one or many likelihood criteria. One likelihood criterion is established by one or many risk management strategies.
Should take account of	Risk Management Plan – Impact criteria	A risk management plan should take account of one-to-many impact criteria. One impact criterion can be linked to many risk management plans.
Takes account of	Risk management plan – Risk factor	A risk management plan takes account of many risk factors. A risk factor is considered by one or many risk management plans.
Will need to be set	Risk management strategy – Scale	A risk management strategy will need to be set at one-to-many scales. A scale is established by one or many risk management strategies.

4.1.3 Risk Profile Management Ontology (RPMO).

4.1.3.1 Purpose.

This subontology provides the key elements to support the RM process in an organisation, through the management of the risk profile (see Figure 4), which is composed of: (i) the recording of the materialisation of the risk, by including the factors that influence the occurrence of a risk event, their causes and consequences, on the objectives of an asset of the organisation, (ii) the description of the results of the risk analysis and the prioritisation of the response to the risk, and (iii) the design of a risk action plan to reduce or eliminate the negative consequences or enhance the opportunities. Therefore, the RPMPO subontology should provide answers to the following CQs:

- CQ11: What risks have been identified for any given asset of the organisation, to which category do they belong, and who owns them?
- CQ12: Which triggers are being used to anticipate the occurrence of the identified risks for any given asset of the organisation?
- CQ13: What are the causes that lead to a risk and what possible consequences could they trigger?

- CQ14: What assets have been impacted by the materialisation of a risk and what are their consequences on the objectives?
- CQ15: What actions help to counteract a risk?
- CQ16: What is the response to risk events that materialise a risk?
- CQ17: What are the causes and risk factors that may influence in the materialisation of a risk?

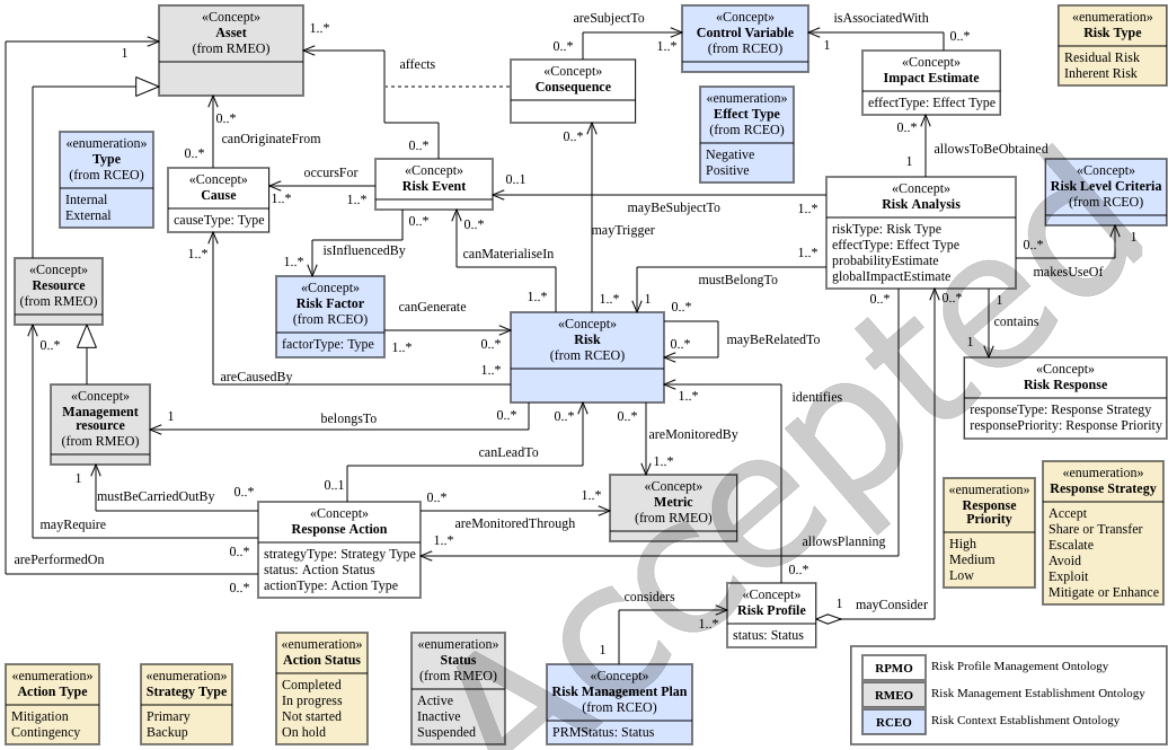

Figure 4: UML representation of Risk Profile Management Ontology (RPMO).

4.1.3.2 *Concepts and relationships of RPMO.*

The precise definitions of the concepts included in the ontology are presented in Table 8. The relationships between these concepts are shown in Table 9.

Table 8: Definition of the terms in the RPMO

Term	Super-concept	Definition	Source
Cause	Concept	Any internal or external factor that has the potential to generate a risk. The causes can be human or non-human, i.e., it can be a process, a management resource, the market, competitors, natural phenomena, etc.	Adapted from: COBIT 5 for Risk [52], PMI [102]
Consequence	Concept	Effects on the objectives of an asset of the organisation caused by the materialisation of a risk. For example, in a project this consequence may be seen on the cost, time, quality, etc.	Adapted from: COBIT 5 for Risk [52], PMI [102]
Impact estimate	Concept	Enables the consequences of a risk event on the organisation's assets to be assessed using impact criteria. It also allows one to determine the effect (positive/negative) of the risk event on the objectives, which are represented by each of the control variables defined by the organisation.	Adapted from: 16085:2021 [68]
Response action	Concept	Specific action that aims to reduce the causes and consequences of a risk to the minimum or to enhance opportunities to the benefit of the organisation. They are carried out by management resources and must be monitored to verify their effectiveness. The response actions once implemented, if not effective, may generate additional risks. The response actions which can be planned by an organisation to manage risks are those of mitigation and contingency. The former ones are aimed at reducing the occurrence or materialisation of risk and the latter ones seek to correct any occurrence of a risk event when the attempts at mitigation have failed.	Adapted from: PMBOK 6th ed. [104], PMI [102], Falbo et al. [27]
Risk analysis	Concept	Risk analysis aims to estimate the probability and impact of risk events in order to understand their effect on the achievement of the objectives and to determine the level of inherent or residual risk after the implementation of the responses defined in the action plan.	Adapted from: COBIT 5 for Risk [52], CMMI V2.0 [17]
Risk event	Concept	Anything that can occur at any specific time and moment, which can have various causes and consequences that can impact the achievement of the objectives of an organisation's assets, having positive or negative effects.	Adapted from: COBIT 5 for Risk [52], ISO 31000:2018 [71]
Risk profile	Concept	It provides the identification and description of the whole set of key risks to which an asset of the organisation is exposed. In other words, all the risks that affect the achievement of the objectives of an asset and which can be generated in the internal context of the organisation in the same way as those that arise in an external context.	Adapted from: 16085:2021 [68]
Risk response	Concept	The response established by the organisation to counteract the risk once it has been assessed. The risk response may have several options (accept, share or transfer, escalate, avoid, etc.) and priorities (high, medium, low), which will be selected in accordance with the magnitude of the risk.	Adapted from: COBIT 5 for Risk [52]

Table 9: Relationships in the RPMO

Name	Concepts	Description
Affects	Risk event – Asset	A risk event affects one or more assets. An asset can be affected by many risk events.
Allows planning	Risk analysis – Response action	A risk analysis allows planning one or many response actions. A response action can be planned in one or many risk analyses.
Allows to be obtained	Risk analysis – Impact estimate	A risk analysis allows many impact estimates to be obtained. Each impact estimate is related to a risk analysis.
Are caused by	Risk – Cause	Many risks are caused by one or many causes. One cause can lead to one or many risks.
Are monitored through	Response action – Metric	Many response actions are monitored through one or many metrics. One metric allows several response actions to be monitored.
Are performed on	Response action – Asset	All the response actions are performed on one or more assets. An asset may or may not require several response actions.
Are subject to	Consequence – Control variable	All the consequences are subject to one or many control variables. A control variable can be considered in several consequences.
Can lead to	Response action – Risk	A response action can lead to many risks. A risk may have been generated by a response action.
Can materialise in	Risk – Risk event	A risk can materialise in many risk events. A risk event is the materialisation of one or many risks.
Can originate from	Cause – Asset	One cause can originate from many assets. One asset can be involved in several causes.
Considers	Risk management plan - Risk profile	Each risk management plan considers one or many risk profiles. Each risk profile is associated with a risk management plan.
Contains	Risk analysis – Risk response	A risk analysis contains a risk response. A risk response is to a risk analysis.
Identifies	Risk profile - Risk	A risk profile identifies one or more risks. A risk can be assigned to one or many risk profiles.
Is associated with	Impact estimate – Control variable	An impact estimate is associated with a consequence. One control variable can be associated with many impact estimates.
Is influenced by	Risk event - Risk factor	A risk event is influenced by one or many risk factors. One risk factor can influence many risk events.
Makes use of	Risk analysis – Risk level criteria	A risk analysis makes use of risk level criteria. Risk level criteria can be used in several risk analyses.
May be subject to	Risk analysis – Risk event	A risk analysis may be subject to a risk event. A risk event is the subject of one risk analysis.
May consider	Risk profile – Risk analysis	A risk profile may consider one or many risk analyses. A risk analysis belongs to a risk profile.
May require	Response action – Resource	A response action may require several resources. One resource may be required in several response actions.
May trigger	Risk – Consequence	A risk may trigger many one or many consequences. A consequence is associated with one or many risks.
Must be carried out by	Response action – Management resource	Each response action must be carried out by a management resource. One management resource can perform many response actions.
Must belong to	Risk analysis - Risk	Each risk analysis must belong to a risk. A risk can be associated with many risk analyses.
Occurs for	Risk event – Cause	A risk event occurs for many causes. A cause can lead to one or many risk events.

4.2 Instance of SRMO

This section presents an example of an application with which the SRMO has been instantiated by considering some of its key concepts (represented by italics in the description of the example). This application example aims to illustrate

some of the benefits of the ontology and the contribution it makes in supporting the RM practices in an organisation. For this purpose, a hypothetical scenario has been created in which real situations are considered, obtained from different RM approaches and from the scientific literature associated with this field of knowledge.

4.2.1 Ontology instantiation example.

Nowadays, organisations support their activities (i.e., operational, financial, strategic, etc.) through a project-based approach, to create new products or services [86,88], as well as to face the continuous market changes and requirements related to technological advances, competition, regulations, economic demands, etc. [79]. This has led to projects becoming a primary business asset to help organisations break out of their status quo and to provide financial and social value [106]. In this regard, RM becomes an essential practice to help organisations and the different parties involved in the *project* to identify *risks* and systematically apply *strategies*, so reducing the negative effects of *risk* on the achievement of the *project objectives*. Accordingly, this is how, using the SRMO, the main elements are put forward for the establishment and support of a "*Risk Management Strategy*" (*RMS*). By means of this *RMS* an organisation can: (i) define a general *policy* for the management of *risk* in *projects*, which should be in line with the needs of the business, (ii) establish the key *objectives* and *metrics* to carry out the measurement and evaluation of the efficacy of the *RMS*, (iii) consider an *approach* for the RM (made up of *categories*, *processes*, *activities*, *tasks* and *artefacts*) which can be adapted to the characteristics of the *projects* and which ensures that the RM is applied in the correct manner, (iv) identify or define the key *management resources* (*organisational roles* and *structures*) to support the practices of the RM with its different levels of *responsibility* and (v) guarantee the regularity of the monitoring and evaluation of the *RMS* by means of the *control points*. In Table 10 an example is shown of the instantiation of each of these concepts, by means of some of the components proposed in the COBIT framework [56].

Table 10: Instance of risk management strategy based on COBIT

SRMO Concept	Instance
Risk Management Strategy	***RMS1***: Risk Management Strategy for programs/projects
Risk Policy	***RP1***: Program/project management policy: Deals with managing risk linked to projects and programs. It details management's position and expectations regarding program and project management. Moreover, it also handles accountability, goals and objectives regarding performance, budget, risk analysis, reporting and mitigating adverse events during the execution of programs and projects.
Metric	***Metric1***: Percent of critical business objectives and services covered by risk assessment ***Metric2***: Ratio of significant incidents that were not identified in risk assessments vs. total incidents ***Metric3***: Frequency of updating risk profile
Objective	***EG02***: Managed business risk. This objective is measured by the ***Metric1***, ***Metric2*** and ***Metric3***
Category	***Category1***: Evaluate, Direct and Monitor
Process	***RMProcess***: Risk Management Process (Adapting COBIT-2019)
Activity	***EDM03***: Ensured Risk Optimisation
Task	***EDM03.01***: Evaluate risk management.
Step	***EDM03.01.1***: Understand the organisation and its context related to I&T risk.
Artefact	***Artefact1***: Evaluation of risk management activities
Role	***Role1***: Chief Risk Officer
Organisational Structure	***OS1***: Enterprise Risk Committee
Responsibility	The ***Role1*** and ***OS1*** are ***Responsible*** for the *task* "***EDM03.01***"
Control Point	The ***RMS1*** should be reviewed and evaluated once annually following its implementation.

An organisation to conduct the RM should define and establish the different criteria or parameters of the risk (i.e., *impact criteria and likelihood criteria*) which should support decision making during the evaluation and prioritisation of the *risks* in the *projects*. These *criteria* reflect the risk appetite that an organisation is willing to take in its pursuit of the *objectives* of the *project*, and should be oriented towards *time*, *scope*, *cost* and *quality*. These objectives make up the so called "triangle" of project management and in the ontology can be defined by means of the concept "*Control Variable*". On the other hand, an organisation should make available the means necessary to carry out the identification and classification of the *risks*. A common way used by organisations is the Risk Breakdown Structure (RBS), which can be generic or specific, according to the type of *project*. In terms of definition, the ontology supplies

the concept of "*Risk Category*". Lastly, each one of these elements and others besides can be included in the *risk management plan*. These elements help to structure and guide the RM practices throughout the entire life cycle of the *project*. In Table 11 one can see an example of each of these concepts, by means of the adaptation of the proposals in the PMBOK [104].

Table 11: Instance of some key elements of a risk management plan based on PMBOK

SRMO Concept	Instance
Scale	***Scale5***: Very High, ***Scale4***: High, ***Scale3***: Medium, ***Scale2***: Low, ***Scale1***: Very Low
Control Variable	***CV1***: Time, ***CV2***: Scope, ***CV3***: Cost, ***CV4***: Quality
Impact Criteria	The **Impact** Type is **quantitative** and is used to estimate risk with **Negative effect** ***IC5***: Impact Rating (Value=5, ***Scale5***), criteria: >20% CV3 increase ***IC4***: Impact Rating (Value=4, ***Scale4***), criteria: 10 to 20% CV3 increase ***IC3***: Impact Rating (Value=3, ***Scale3***), criteria: 3 to 10% CV3 increase ***IC2***: Impact Rating (Value=2, ***Scale2***), criteria: 1 to 3% CV3 increase ***IC1***: Impact Rating (Value=1, ***Scale1***), criteria: <1% CV3 increase
Likelihood Criteria	Criteria used to estimate the **likelihood** of risk with **negative effect** ***LC5***: Likelihood Rating (Value=5, ***Scale5***), criteria: >70% ***LC4***: Likelihood Rating (Value=4, ***Scale4***), criteria: 40-70% ***LC3***: Likelihood Rating (Value=3, ***Scale3***), criteria: 20-40% ***LC2***: Likelihood Rating (Value=2, ***Scale2***), criteria: 5-20% ***LC1***: Likelihood Rating (Value=1, ***Scale1***), criteria: 0-5%
Risk level Criteria	Criteria used for the classification of **level of risk** with **negative effect** ***RL4***: criteria: risk magnitude >=60, ***Scale5*** ***RL3***: criteria: risk magnitude > 40 and <60, ***Scale4*** ***RL2***: criteria: risk magnitude >12 and <40, ***Scale3*** ***RL1***: criteria: risk magnitude <=12, ***Scale2***
Risk Category	***RC1***: Project Risk (Risk Category) |_ ***RC1.1***: Technical Risk (subcategory) |_ ***RC1.1.2***: Requirements definition (subcategory)

The risks can be generated by different factors and at different stages of the project. Accordingly, it is important to carry out an adequate identification and register of the risks by means of a risk profile of the project. A basic example of a risk register can be seen in Table 12.

Table 12: Instance of risk register in projects

SRMO Concept	Instance
Project	***Project001***
Risk Profile	The risk profile defined for ***Project001*** is the ***RProfileProject001*** and the risk identified is ***R001***.
Risk Factor Category	***RFC1***: Risk factors of project (**Risk Factor Category**) |_***RFC1.1***: Product engineering (**subcategory**) |_***RFC1.1.1***: Requirements (**subcategory**) *Note: The risk factor categories are based on those proposed in* [83]*, which are concerned with software development projects.*
Risk Factor	***RF1***: Requirement ambiguity, Type **Internal** and ***RF1*** is classified in ***RFC1.1.1***.
Role	***Role2***: Project Manager ***Role3***: Business Analyst
Metric	***Metric7***: Check that the specification of the project requirements complies with 100% of the characteristics described in the requirements quality model defined/used by the organisation (**Risk Trigger**). ***Metric8***: Check that 100% of the requirements can be implemented and are actually necessary for the project (***Risk Trigger***). ***Metric9***: Approval by the client of the specification of the requirements (***Risk Trigger***). ***Metric10***: Percent of requirements changed during project execution (***Risk Trigger***).
Risk	***R001***: Poor Requirements Quality. The ***R001*** belongs to the ***Role2*** (**risk owner**) and this is generated by ***RF1***. The risk pertains to ***RC1.1.2*** and the risk triggers associated are ***Metric7***, ***Metric8***, ***Metric9*** and ***Metric10***.
Cause	***Cause1***: Lack of ability among the requirements engineers. This cause can generate the ***R001*** risk. ***Cause2***: Lack of commitment from the client/end user to provide information on the project requirements. This cause can generate the ***R001*** risk.
Consequence	***Cons1***: Failure to meet the agreed delivery dates for products. The ***Cons1*** is subject to ***CV1*** and can be caused by ***R001*** risk. ***Cons2***: Increases in the project budget to be assumed by the organisation. The ***Cons2*** is subject to ***CV3*** and can be caused by ***R001*** risk.
Risk Analysis	***RA001***, Risk Type: **Inherent Risk** The project risk team determined that the approximate estimate of the **likelihood** of the occurrence of the risk is 5, and that the approximate global estimate of how significant the risk **impact** would be, if it happened and thus became an issue, is 18. Finally, the **risk magnitude** is 90, therefore, the risk level is ***RL4***.
Impact Estimate	The approximate estimate of the risk impact ***R001***, in relation to the objectives of the project represented by the control variables: ***IE1***: ***CV1***, Score=5, ***IE2***: ***CV2***, Score =4, ***IE3***: ***CV3***, Score =5, ***IE4***: ***CV4***, Score =4 The total of the estimate of the risk impact is 18.
Risk Response	The decision made to respond to the ***R001*** risk is mitigate (**Response Strategy**)
Response Action	The response actions planned to help in mitigating the ***R001*** risk analysed via the ***RA001***, and which should be carried out

by ***Role3***, are:
RAction1: Train the requirement engineers or system analysts about the business logic of the project that is to be developed.
RAction2: Ensure that the users are clear as to what they want to achieve with the project.

4.3 Implementation of the SRMO

This ontology was implemented in OWL (Ontology Web Language) [130], using the Protégé editor [90] (5.5.0 version). This editor enables the construction of ontologies based on frames. As a result, each of the SRMO concepts was transformed into a class, each of the attributes into data properties through domains, and each of the relationships into object properties. It is also worth mentioning that the enumerations were transformed as data properties, using the ranges, by assigning the values predefined in the subontologies.

In addition, to enable the evaluation of the ontology and the execution of the CQs, the instance of SRMO (section 4.2) was populated and completed by creating a series of instances/objects in each of the classes, which are referred to in Protégé as individuals. A summary of this implementation can be observed in Table 13 and in Figure 5, which show the obtained values of the key metrics generated by the tool.

Table 13: Ontology metrics

Metrics	Results
Axiom	2118
Logical axiom count	1656
Declaration axioms count	462
Class count	46
Object property count	99
Data property count	44
Individual count	273

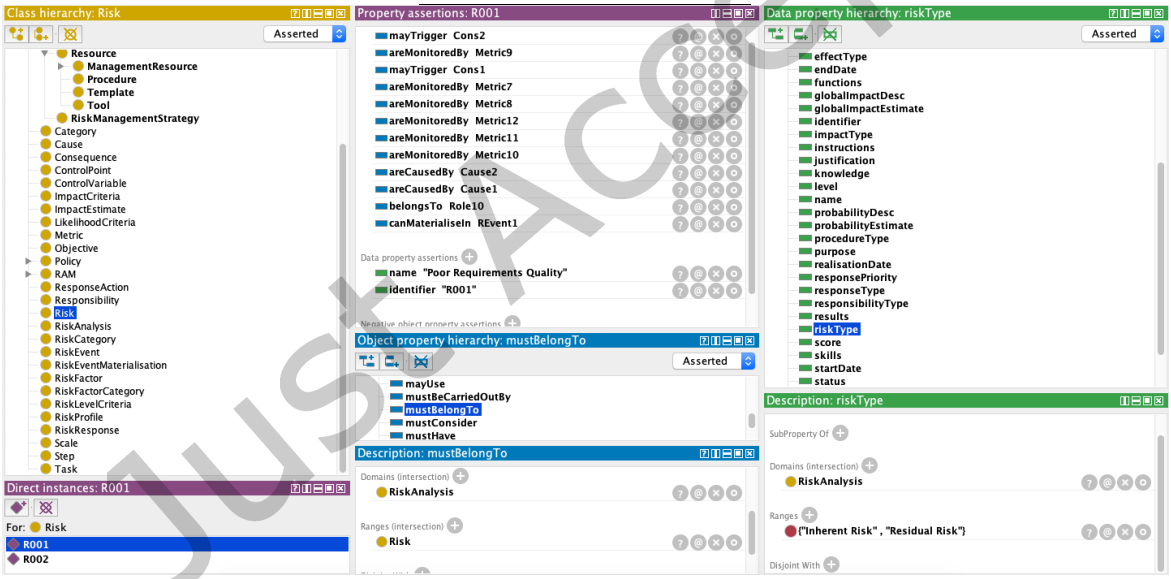

Figure 5: The screenshot of the ontology implemented in Protégé.

4.4 Application of the Competency Questions to the SRMO

Competency questions (CQs) are used to evaluate ontological commitments and to determine whether an ontology meets the requirements [42,92]. In order to perform this check and verify whether the ontology can work in a real world, a formal specification of the CQs was performed manually, using the SPARQL query language [131] and tested

with the Protégé tool. It should be noted that the CQs were applied to the ontology instance described in section 4.3. A summary of the formalisation of the CQs is shown in Table 14. The answers given by each of the CQs can be found in the ontology resources repository (see section 5.2.2).

Table 14: Competency questions expressed in SPARQL

#	Specific Competency Question	SPARQL Query

CQ1	What are the established objectives and metrics for the risk management strategy for programs/projects "RMS1"?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?O ?M
		WHERE {
		?RMS SRMO:mustHaveAssigned ?O.
		?O SRMO:isMeasuredBy ?M.
		?RMS SRMO:identifier "RMS1"
		}

CQ2	What are the RM process tasks associated with the risk management strategy for programs/projects "RMS1", what are the management resources allocated to them, and what is their accountability?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?P ?T ?MR ?R
		WHERE {
		?P SRMO:consistsOf ?A.
		?A SRMO:canBeSubdividedInto?T.
		?RAM_Task SRMO:mustSetOut ?T .
		?RAM_Task SRMO:mustSpecify ?MR.
		?RAM_Task SRMO:provides ?R .
		?RMS SRMO:mustStipulate ?RAM_Task .
		?RMS SRMO:identifier "RMS1".
		}

CQ3	What are the objectives and metrics assigned to the RM process "RMProcess"?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?P ?O ?M
		WHERE {
		?P SRMO:mustHaveAssigned ?O.
		?O SRMO:isMeasuredBy ?M.
		?P SRMO:identifier "RMProcess".
		}

CQ4	What are the procedures that can be used in the RM process tasks "RMProcess"?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?P ?A ?Pr
		WHERE {
		?P SRMO:consistsOf ?A.
		?A SRMO:canBeSubdividedInto ?T.
		?T SRMO:canUse ?Pr.
		?P SRMO:identifier "RMProcess"
		}

CQ5	What are the active risk management strategies, what scope do they have, and through what approach are they implemented?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?RMS ?App
		WHERE {
		?RMS SRMO:hasAsItsScope ?A .
		?RMS SRMO:areManagedWith ?App.
		?RMS SRMO:status "Active".
		}

CQ6	What are the identified risk categories and subcategories in the risk management strategy for programs/projects "RMS1"?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?rC ?sbRCL1 ?sbRCL2
		WHERE {
		?rC SRMO:mayHave ?sbRCL1.
		?sbRCL1 SRMO:mayHave ?sbRCL2.
		?RMS SRMO:shouldIdentify ?rC.
		?RMS SRMO:identifier "RMS1".
		}

CQ7	What assets of the organisation are implementing the risk management strategy for programs/projects "RMS1"?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?A ?RMP ?RMS
		WHERE {
		?A SRMO:canContain ?RMP.
		?RMP SRMO:shallConsider ?RMS.
		?RMP SRMO:status "Active".
		?RMS SRMO:identifier "RMS1".
		}

CQ8	What are the acceptance criteria defined in the risk management strategy for programs/projects "RMS1" and which are considered by an asset of the "Project - Project001" organisation?	PREFIX SRMO: <http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#> SELECT ?aC WHERE { ?RMP SRMO:hasRelated ?aC. ?A SRMO:canContain ?RMP. ?RMP SRMO:status "Active". ?A SRMO:identifier "Project001"

		}
		PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?rF ?R
		WHERE {
		?A SRMO:canContain ?RMP.
		?RMP SRMO:takesAccountOf ?rF.
		?rF SRMO:canGenerate ?R.
		?rC SRMO:canClassify ?R.
		?RMP SRMO:status "Active".
		?A SRMO:identifier "Project001".
		}

CQ9	What risk factors are taken into account by an asset of the "Project - Project001" organisation and what risks do they cause?	

CQ10	What impact criteria are related to an asset of the "Project - Project001" organisation and with which control variables are they associated?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?iC ?eT ?cV ?S
		WHERE {
		?A SRMO:canContain ?RMP.
		?RMP SRMO:shouldTakeAccountOf ?iC.
		?iC SRMO:require ?S.
		?iC SRMO:hasAssociated ?cV.
		?iC SRMO:effectType ?eT.
		?RMP SRMO:status "Active".
		?A SRMO:identifier "Project001".
		}

CQ11	What risks have been identified for an asset of the "Project – Project 001" organisation, to which category do they belong, and who owns them?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?R ?rC ?mR
		WHERE {
		?A SRMO:canContain ?RMP.
		?RMP SRMO:considers ?rP.
		?rP SRMO:identifies ?R.
		?rC SRMO:canClassify ?R.
		?R SRMO:belongsTo ?mR.
		?rP SRMO:status "Active".
		?RMP SRMO:status "Active".
		?A SRMO:identifier "Project001".
		}

CQ12	What triggers are being used to anticipate the occurrence of the identified risks for an asset of the "Project – Project 001" organisation?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?R ?M
		WHERE {
		?A SRMO:canContain ?RMP.
		?RMP SRMO:considers ?rP.
		?rP SRMO:identifies ?R.
		?R SRMO:areMonitoredBy ?M.
		?rP SRMO:status "Active".
		?RMP SRMO:status "Active".
		?A SRMO:identifier "Project001".
		}

CQ13	What are the causes that generate an "Poor Requirements Quality (R001)" risk, and what possible consequences could it trigger?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?cons ?cause
		WHERE {
		{
		?R SRMO:areCausedBy ?cause.
		?R SRMO:identifier "R001".
		}
		UNION
		{
		?R SRMO:mayTrigger ?cons.
		?R SRMO:identifier "R001".
		}
		}

CQ14	What assets have been impacted by the materialisation of a "Poor Requirements Quality (R001)" risk and what are their consequences on the objectives?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?a ?cons ?cV
		WHERE {
		?R SRMO:canMaterialiseIn ?rE.
		?rE SRMO:effects ?REM.
		?REM SRMO:affects ?a.
		?REM SRMO:results ?cons.
		?consq SRMO:areSubjectTo ?cV.
		?R SRMO:identifier "R001"
		}

CQ15	What actions help to counteract a "Poor Requirements Quality (R001)" risk?	PREFIX SRMO: <http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#> SELECT ?rAction ?aT WHERE { ?rA SRMO:mustBelongTo ?r. ?rA SRMO:allowsPlanning ?rAction. ?rAction SRMO:actionType ?aT. ?r SRMO:identifier "R001"

		}
		PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?rE ?rA ?rR
		WHERE {
		?r SRMO:canMaterialiseIn ?rE.
		?rA SRMO:mayBeSubjectTo ?rE.
		?rA SRMO:mustBelongTo ?r.
		?rA SRMO:contains ?rR.
		?r SRMO:identifier "R001".
		}

CQ16	What are the responses to risk events that materialise in a "Poor Requirements Quality (R001)" risk?	

CQ17	What are the causes and risk factors that may influence in the materialisation of a "Poor Requirements Quality (R001)" risk?	PREFIX SRMO:
		<http://www.semanticweb.org/jhonmassodaza/ontologies/2021/0/SRMO#>
		SELECT ?c ?rF
		WHERE {
		{
		?r SRMO:canMaterialiseIn ?rE.
		?rE SRMO:occursFor ?c.
		?r SRMO:identifier "R001".
		}
		UNION
		{
		?r SRMO:canMaterialiseIn ?rE.
		?rE SRMO:isInfluencedBy ?rF.
		?r SRMO:identifier "R001".
		}
		}

5 EVALUATION OF THE SRMO

In this section the evaluation of the SRMO ontology is addressed, which is a key task in the process of building and refining an ontology [39,77] which is reliable, so it can be shared and used by the community [129]. According to McDaniel et al. [82], the evaluation applied to a domain ontology aims to assess whether an ontology has been accurately, efficiently and adequately modelled with respect to the domain it represents. The authors propose a framework called the "Ontology Evaluation Pipeline", which combines different evaluation methods and approaches available in the literature. This framework aims to make an ontology which is error-free, modular in nature, and which can be stored in an ontology repository so that it can be easily found and shared. The evaluation set out in the framework comprises two phases, ontology validation and ontology improvement, whose application for the SRMO is described in the following subsections. In addition to this evaluation, the use of the ontology is presented through two scenarios or application cases.

5.1 Ontology Validation Phase

The ontology validation purpose is to verify that an ontology is of sufficient quality to be used and also that it is appropriate for the domain it represents [82]. To carry out this phase, three activities are suggested: (i) check domain and task fitness, (ii) remove errors and (iii) apply metrics.

5.1.1 Check Domain and Task Fitness.

This activity is designed to verify if the ontology meets the domain objectives and for this purpose, the FOCA methodology [6] was selected, as it enables quality control of the ontology. FOCA uses a questionnaire that follows the GQM approach to evaluate the components of the ontology along with a statistical model for the calculation and verification of the ontology quality. FOCA consists of three steps: (i) ontology type verification, (ii) questions verification and (iii) quality verification. One expert in ontologies, projects management and software processes manually reviewed the SRMO and applied the method described below.

5.1.1.1 *Step 1- Ontology Type Verification.*

The type of ontology must be specified in this step for which the following FOCA verification types are: Type1 - Domain or Task ontology; and Type 2 - Application ontology). As mentioned above, the SRMO is considered as a domain ontology.

5.1.1.2 *Step 2- Questions Verification.*

Table 15 contains a summary of how GQM was applied for this step. This consists of five objectives, thirteen questions and six metrics, which allow the quality of an ontology to be evaluated. It is also worth mentioning that the methodology specifies that depending on the type of ontology a question will be disabled. Since SRMO is a domain ontology, question Q4 should not be considered. On the other hand, each question should have a score associated to it. To award this score, the authors [6] define for each one of the questions specific verification criteria, which will allow one to evaluate whether or not the ontology fulfils the purpose of the question, through the assignment of a corresponding value (e.g., 25, 50, 75, 100). Finally, the average of each of the objectives is calculated, with reference to the scores achieved by each of the questions that are associated to the objectives.

Table 15: Applying the GQM approach of the FOCA methodology on the SRMO

Goal	Question	Metric	Grade	Mean
1. Check if the ontology complies with Substitute	Q1. Were the competency questions defined?	1. Completeness	100	66.66
	Q2. Were the competency questions answered?	1. Completeness	100	
	Q3. Did the ontology reuse other ontologies?	2. Adaptability	0	
2. Check if the ontology complies Ontological Commitments	Q4. Did the ontology impose a minimal ontological commitment?	3. Conciseness	-	75
	Q5. Did the ontology impose a maximum ontological commitment?	3. Conciseness.	50	
	Q6. Are the ontology properties coherent with the domain?	4. Consistency	100	
3. Check if the ontology complies with Intelligent Reasoning	Q7. Are there contradictory axioms?	4. Consistency	100	100
	Q8. Are there redundant axioms?	3. Conciseness	100	
4. Check if the ontology complies Efficient Computation	Q9. Did the reasoner bring modelling errors?	5. Computational efficiency	100	100
	Q10. Did the reasoner perform quickly?	5. Computational efficiency	100	
5. Check if the ontology complies with Human Expression	Q11. Is the documentation consistent with modelling?	6. Clarity	100	100
	Q12. Were the concepts well written?	6. Clarity	100	
	Q13. Are there annotations in the ontology that show the definitions of the concepts?	6. Clarity	100	

5.1.1.3 *Step 3- Quality Verification*

In this step the quality of the ontology must be calculated. The authors in [82] propose two ways to carry out this calculation, which are called total quality and partial quality. For this paper the total quality verification was selected since this method allows one to consider the five roles for knowledge representation (i.e., Substitute, Ontological Commitments, Intelligent Reasoning, Efficient Computation and Human Expression). These roles are related to the five objectives presented in Table 15. The total quality of the ontology is calculated using the beta regression model (see equation 1) proposed by Ferrari et al. [33]. The result of applying this model ranges between 0 and 1.

$$\widehat{\mu_i} = \frac{exp\left(-0.44+0.03(Cov_S \; x \; Sb)_i+0.02(Cov_C \; x \; Co)_i+ 0.01(Cov_R \; x \; Re)_i \; +0.02\left(Cov_{Cp} \; x \; Cp\right)_i-0.66LExp_i-25(0.1x \; Nl)_i\right)}{1+exp\left(-0.44+0.03(Cov_S \; x \; Sb)_i+0.02(Cov_C \; x \; Co)_i+ 0.01(Cov_R \; x \; Re)_i \; +0.02\left(Cov_{Cp} \; x \; Cp\right)_i-0.66LExp_i-25(0.1x \; Nl)_i\right)} \quad (1)$$

Criteria to calculate the total quality:

- $\mathrm{Cov_S}$ is the mean of grades obtained from Goal 1.
- $\mathrm{Cov_C}$ is the mean of grades obtained from Goal 2.
- $\mathrm{Cov_R}$ is the mean of grades obtained from Goal 3.
- $\mathrm{Cov_{Cp}}$ is the mean of grades obtained from Goal 4.
- LExp is the variable which corresponds with the experience of the evaluator. If the evaluator considers himself/herself a person with vast experience in ontologies, the value of LExp is 1, if not, 0;

- Nl is 1 only if some Goal was impossible for the evaluator to answer all the questions;
- Sb = 1, Co = 1, Re = 1, Cp = 1, because the total quality considers all the roles.

Substituting the values obtained after applying the questionnaire (see Table 15) in the beta regression model (equation 1) and the criteria to calculate the total quality, results in:

$$\hat{\mu} = \frac{exp(-0.44 + 0.03(66.66\ x\ 1) + 0.02(75\ x\ 1) + \ 0.01(100\ x\ 1) + 0.02(100\ x\ 1) - 0.66\ x\ 0\ - 25(0.1x\ 0))}{1 + \ exp(-0.44 + 0.03(66.67\ x\ 1) + 0.02(75\ x\ 1) + \ 0.01100\ x\ 1 + 0.02(100\ x\ 1) - 0.66\ x\ 0\ - 25(0.1x\ 0))}$$

$$\hat{\mu} = \frac{exp(-0.44\ +\ 1.9998\ + 1.5\ +\ 1\ +\ 2\ -\ 0 - 0)}{1 + \ exp(-0.44\ +\ 1.9998\ + 1.5\ +\ 1\ +\ 2\ -\ 0 - 0)}$$

$$\hat{\mu} = \frac{exp(6.0598)}{1 + \ exp(6.0598)} = 0.997670571$$

The result of the total quality is 0.997and being a result close to 1 one can conclude that the SRMO is of a high quality.

5.1.2 Remove Errors.

This activity is aimed at eliminating syntactic errors and inconsistencies in verification and at reducing redundancies. In order to carry out this activity, the Ontology Taxonomy Evaluation method was applied [77]. This is a manual evaluation method for verifying errors in the construction of the taxonomic knowledge of the frames-based ontology [39,77]. It rests on three main criteria: Inconsistency, Incompleteness and Redundancy. The application to the ontology of these criteria is shown in Table 16.

Table 16: Ontology taxonomy evaluation

Criteria	Subcriteria	Explanation
Inconsistency	Circularity errors Partition errors Semantic errors	In order to validate semantic inconsistencies in the ontology, a review of each of its concepts and subconcepts was carried out, as well as its instances. It could be verified that there were no circularity errors between the concept relationships and partitioning errors. The Hermit reasoner was also used to find inconsistencies.
Incompleteness	Incomplete concept classification Partition errors	The integrity of the concepts and their relationships was assessed, verifying that the domains and ranges of relationships were appropriate and accurate and that the class properties represented the basic and necessary information to understand the domain concepts. In addition, all the concepts specified in the ontology design were included.
Redundancy	Grammatical redundancy Identical formal definition of some classes Identical formal definition of some instances	It could be verified that there were no redundancy or incompleteness errors in the defined concepts of the ontology, nor in their representation by means of classes, the latter in order to eliminate possible ambiguities.

5.1.3 Apply Metrics.

Once it has been established that the ontology matches the domain for which it was designed, metrics must be applied to verify or check its quality [82]. For this purpose, the five basic criteria to evaluate the quality of an ontology identified by Gomez-Perez [39] were used: consistency, completeness, conciseness, expandability and sensitiveness. The application of these criteria, which are shown in Table 17, will ensure that the ontology is correctly constructed with respect to the content it represents.

Table 17: Ontology quality criteria

Criteria	Explanation
Consistency	We can assert that the description of the ontology and subontologies is consistent since they are aligned with the domain they represent. Furthermore, the document presents the definition of each of its terms and their relationships, to avoid contradictions and misinterpretations. The definition of its terms arises from the analysis, and comparison of the associated terminology in widely recognised RM standards and frameworks. For the graphic representation, the SRMO uses a basic notation (UML class diagrams), which could aid a better understanding of the knowledge modelled, as UML is a language widely used by industry and academia. Tests were also conducted to validate the consistency of the knowledge modelled and implemented in Protégé, using the Hermit reasoner, to ensure that the ontology did not present errors. This is to ensure that the ontology is error-free and complies with the domain specifications. Finally, examples of instantiation were made to demonstrate how each of the concepts can be used.
Completeness	The ontology tries to adequately cover the whole context of RM from an integrated approach, providing the key elements that enable the establishment of an RMS supported by decision-making mechanisms and a holistic risk management. In this sense, the ontology includes the most relevant terms to facilitate the understanding and comprehension of this management practice. Each of these terms was organised in tables, accompanied by their definition and bibliographic support. On the other hand, competency questions were defined and adapted by means of test cases to evaluate the fulfilment of the ontology's requirements and to verify that the outputs are correct.
Conciseness	The ontology is concise, as it does not present definitions of unnecessary or irrelevant terms. The ontology does not present redundancies between existing terms and their representations.
Expandability	Since it has not been tailored to specific organisations or management fields, the SRMO can be adapted and extended by including and defining new terms, so that it can be used in specific industry contexts.
Sensitiveness	The ontology is not expected to be sensitive to small changes in the existing definitions. This is because the definitions of its terms have been consistently achieved, through the disciplined integration of the different definitions from the relevant RM standards and frameworks.

5.2 Ontology Improvement Phase

This phase is aimed at further improving the ontology, if necessary, before it can be published, in order to provide an ontology with the necessary quality for its use in the future. To carry out this phase, two activities are set out [82]: (i) Pruning and modularisation and (ii) Library placement.

5.2.1 Pruning and modularization.

The modularisation consists of pruning and modularising the ontology, prior to its publication, i.e., subdividing it into smaller pieces that are easier to use and that have specific purposes with regard to the knowledge they represent. This improvement activity was not applied once the validation phase of the ontology was finished, since originally the SRMO was conceived in a modular way, with specific purpose subontologies that would cover different plots of the RM domain, but which together would support the implementation and execution of this process, providing organisations with an integrated vision of risk. In addition, this modular design of the SRMO facilitates the reuse of knowledge and the updating of each of its terms and relationships. On the other hand, each of the subontologies underwent changes during its design and implementation phase. Therefore, pruning was applied to eliminate unnecessary terms and relationships, to guarantee the purpose of each of the subontologies with respect to their domains and thus avoid redundancies. This made it possible to generate the connections between each of them through relevant terms.

5.2.2 Library placement.

The purpose of this activity is to create or select an appropriate repository for the ontology publication. To fulfil this, the ontology and the competency questions, which were implemented by using the Protégé editor, were placed in the github repository, so that they could easily be accessed and used in future studies through the following URL: http://bit.ly/SRMO_Resources

5.3 SRMO Application Cases

In order to strengthen the evaluation process, this section presents two scenarios or application cases that demonstrate the usefulness and capacity of SRMO in real situations.

5.3.1 Application Case 1: Universidad del Cauca.

This application case aims to demonstrate the usefulness of SRMO to analyse the strategies implemented at the University of Cauca (Unicauca, Colombia) to mitigate risks due to the global situation caused by the COVID-19 pandemic. This pandemic forced social distancing and the closure of the university in order to protect the health and safety of the university community. Unicauca, through the Superior Council, was confronted with the need to respond quickly to this situation by implementing transitory measures to guarantee academic activities and those related to the fulfilment of its mission objectives, through the use of information and communication technologies (ICT) or others that would allow a gradual return to the tasks that were carried out on a daily basis, but in a virtual context. This obliged the Superior Council to carry out an assessment of the risks that the university community could face and to define an action plan to help counteract the challenges arising from this new normality.

This application scenario was carried out with the help of two staff members of the institution, with whom the documentation related to the strategies implemented by the university in the academic context was reviewed and analysed. Through several virtual work sessions, the knowledge used in the strategies was identified according to the ontology developed. For reasons of confidentiality, only some of the results of the analysis which are representative for illustrating the applicability of the ontology are presented here:

- Control actions to reduce risks related to the use of digital platforms and technologies to improve pedagogical resources, academic assessments and online teaching activities, etc, by teachers. In this sense, Unicauca defined different control actions aimed mainly at: (i) training of teachers in the use of information technologies (IT), (ii) acquisition of software products and services in the cloud to support teaching activities and their configuration on the university's platforms, and (iii) adjusting the software of the Integrated System of Enrollment and Academic Control (SIMCA) to adapt and configure it to the current situation.
- Control actions to reduce the risk of dropout of undergraduate students in vulnerable socio-economic situations, internet connectivity problems and lack of computer equipment. In order to strengthen the continuity of students, the university established control measures aimed at: (i) acquisition of computer equipment, extension of software licences and internet data plans, (ii) definition of a protocol for the selection, allocation, monitoring and control of resources, and (iii) implementation of a report in SIMCA for the characterisation of the university population with respect to geographical location, economic situation and socio-economic stratum to help each Faculty Council of the university in the selection and allocation of the different resources.
- Unicauca, being a public entity, has implemented the Risk Management Component, defined in the Internal Control Standard Model (MECI) [87], which is required by the Colombian government for its public entities and is based on the ISO 31000 Standard. Regarding the implementation of this component, it became evident that the university has not updated the RMS to date with respect to the current situation; although there are guidelines through institutional agreements, these have not been included in the RMS. There was evidence of a lack of rigour in the assignment of levels of responsibility for the different management resources identified with the new risk mitigation strategies as a result of COVID-19, as well as those already established at a general level in the RMS. There is a comprehensive institutional risk map in force for 2021, but it has not been updated with the risks identified as a result of COVID-19 and for which mitigation strategies are already in place. It was also possible to observe that the RMS specifies the criteria to support the assessment of risks, but these are very generic. In the case of the criteria for determining impact, only corruption risks are considered, leaving aside other key constraints for the university (i.e., reputational, operational, technological, information,

environmental, etc.). On the other hand, there is a general risk policy and no specific RM guidelines for the most critical assets, which would help to promote and strengthen this management practice.

- It was possible to identify that the university has a Technological Resources Management process, but this has not been included in its critical processes. This process is vital for the functioning of the institution and even more so in the current situation, since among its objectives is the construction of computer applications that contribute to the automation of institutional processes, through the formulation, development and implementation of projects that provide solutions to the problems or needs of the institution.

In summary, this brief application scenario allows us to demonstrate the usefulness of the ontology and to see how it can serve as a tool to help analyse the definition and/or implementation of risk mitigation strategies in an organisation. The main lesson learned from having put this proposal into practice is that an organisation can benefit from an ontology to analyse, verify and validate an RMS, as it offers structured and formalised knowledge that can be adapted to its needs. Moreover, being an ontology that integrates different RM approaches, they can consider other elements that will help to complement or improve an RMS. On the other hand, we are also aware that this application case has limitations that need to be taken into account. We used the SRMO in an organisation that does not belong to the software development sector, but is an institution that depends on software to meet its mission objectives and because of the COVID-19 pandemic accelerated its digital transformation to improve its processes. Additionally, with remote work and online classes, the use of ICT and access to computer applications by the university community increased, bringing with it enormous challenges and risks for the institution. Situations that motivated us to select Unicauca for the application of our ontology. Another limitation is the profile of the staff, as none of them had knowledge of ontologies or knowledge models, which implied active participation in the activity, which could have influenced the results of the analysis. Therefore, a future evaluation of the SRMO should consider ontology and RM experts with different levels of experience. As well as software organisations to be able to instantiate, analyse, validate or verify the definition and implementation of an RMS in companies in this sector.

5.3.2 Application Case 2: Use of the SRMO for the definition of a RM methodology.

The SRMO was used to define a specific RM methodology belonging to a methodological framework aimed at supporting the RM of an organisation's assets from an integrated approach. This methodology describes in detail the activities and tasks to be performed by all stakeholders in RM. In this sense, the SRMO provided the conceptual structure of the RM domain at the different management levels of an organisation, through each of the subontologies (RMEO, RCEO and RPMO). These subontologies resulted in two processes: Establishment of Business Risk Management (EBRM) and Risk Management (RM). For their definition, the process pattern developed in the framework of the COMPETISOFT project [94] was adapted. Furthermore, the definition of the processes is supported by the standard notation of SPEM 2.0 [97] and the use of the modelling tool EPF Composer [23]. An overview of the methodology is presented in Figure 6.

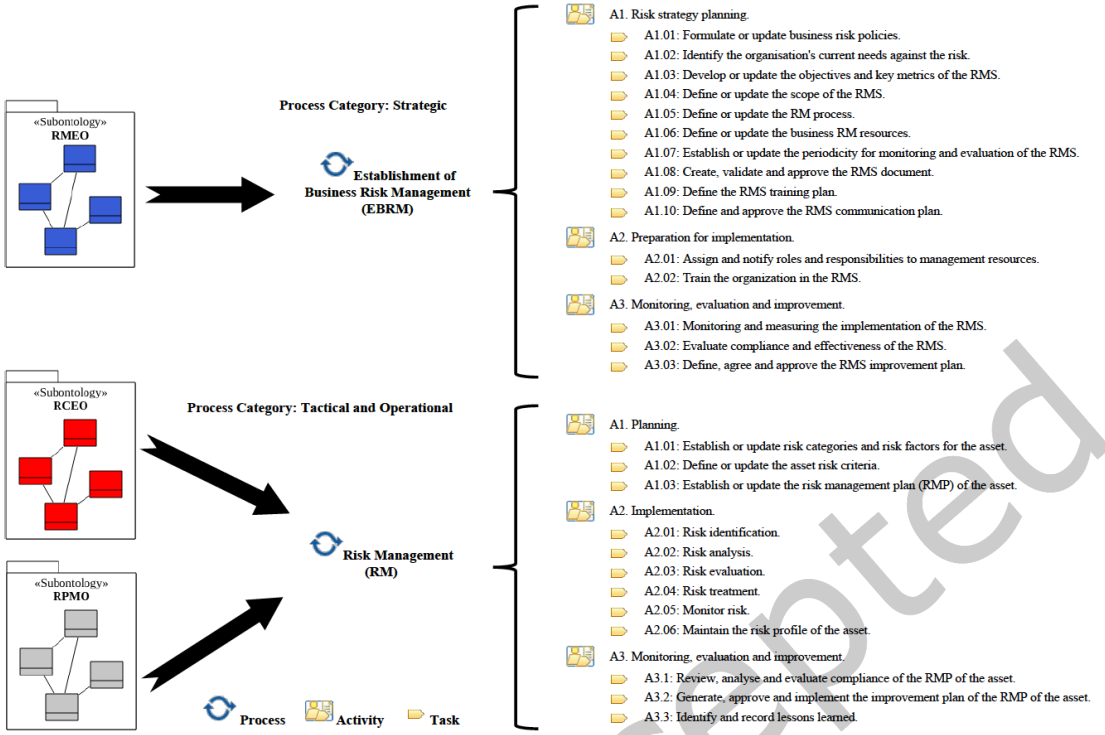

Figure 6: Processes, activities and tasks of the RM Methodology.

Overview of the main processes of the defined RM methodology:

- **EBRM**: This process is oriented at the strategic level of the organisation. It provides a consistent approach to defining and establishing an RMS that is aligned with the governance approach and allows for a holistic view of risk to help preserve the value of the organisation. Through the definition of a risk policy that achieves the organisation's objectives, with clear coverage of the assets to be managed, objectives and key metrics to measure and control the execution of the RMS. It also allows specifying a standard approach to RM with respect to the nature of the business, including the different organisational structures, roles and responsibilities that will address the risks. It furthermore ensures monitoring and evaluation of the RMS to provide results that promote continuous improvement and documentation of lessons learned.
- **RM**: This process is oriented to the tactical and operational level of the organisation and provides the key elements to define and establish the context of RM, through the identification of the different sources and causal factors of risks that have an impact on the assets and that may be in the internal and external context of the organisation. As well as the criteria that will allow decision making at the time of carrying out the risk assessment, regarding the amount and type of risk that an organisation is willing to assume in the fulfilment of its asset objectives. Each of these criteria should be documented in the asset's risk management plan (RMP). This RMP will address the organisation's intent with the RMS and serve as a mechanism to support the implementation of an asset's RM. Through the systematic application of activities and tasks that will support the identification, analysis, assessment, treatment and monitoring of risks. These should be collected, documented

and communicated through appropriate management of the asset's risk profile. The RMP and RM process should be monitored and evaluated to improve its effectiveness.

6 DISCUSSION

As described in Section 2.2, most of the ontologies oriented to the RM domain are based on approaches (models, frameworks, standards, etc.) that have already been withdrawn or replaced by the institutions that publish them. Also, very few reported a formal method for their construction, which together with the shortcomings found regarding the definitions of concepts and their relationships, the use of modelling languages for the representation of the proposals or their implementation through tools, prevented a better analysis and use of the defined knowledge. These situations reveal a dearth of maturity and formality in the development of ontologies [136]. Moreover, they are focused on supporting specific RM activities in various application contexts and with differing degrees/levels of specification, which means that there is still ambiguity and heterogeneity in the terminology associated with this management practice. This situation can also be seen in the different approaches to RM that were analysed for the design of the ontology and which are presented in Section 2.1.

It could also be observed that, at the ontological level, the RM field has not been treated from an integrated approach. Most of the proposals still consider RM from a traditional or tactical approach. For this reason, the present proposal has been designed to support a holistic view of risk that could be adapted to the needs of an organisation. This ontology is intended to provide the key and fundamental elements for organisations to establish an RM that supports their in-house strategy and that allows the creation and preservation of value, through the application of RM practices at any organisational level. In addition, it should provide support to the stakeholders involved in the various RM activities. All of the above, based on a thorough analysis of the most relevant RM approaches and following a rigorous method for its development, which helped to meet the main requirements of the ontology. Additionally, it was implemented using the Protégé tool to check the logic of the knowledge it represents and shared through a web repository, so that it can be tested by other researchers and reused/modified in future research. As a result, it is expected to contribute to closing the gaps in this domain which were detected in the literature review.

On the other hand, as shown in Table 2, only 56,25% of the analysed ontologies present some kind of evaluation and very few follow a formal method that allows each of the steps followed in the evaluation process to be corroborated. Of these studies, 25% (4 studies) report validating their ontology through a case study. However, they do not present or describe the protocol followed, the research question, units and subjects of analysis, validation plan, among others, which shows insufficient rigour in the use of this validation method. Although it should be noted that despite the absence of these elements in [24] the researchers present and discuss the validity threats of their proposal. This evidences the need for a systematic and unique method that can be applied to any type of ontology and that is supported by well-defined and proven theories [82]. Those who design ontologies would undoubtedly be helped by having available to them a systematic method that guarantees the quality of their proposals and which allows them to consider and combine methods that help to evaluate the quality of an ontology from different dimensions. From this perspective, once the SRMO had been designed and implemented, we evaluated its quality by applying different methods contained in the framework proposed by McDaniel et al [82]. The application results obtained demonstrate that the proposal meets several quality and content criteria. This was also corroborated through the FOCA methodology, which was applied by an expert in ontologies, software processes and project management, who also had basic knowledge of RM. The result of this validation determined that the ontology meets quality criteria. We are aware that this result depends on the expertise of the evaluator on the domain and as it was performed by a human, it

may contain biases, but this was a beneficial activity that allowed us to have an external opinion on the quality of our proposal. In a future, the validation of the ontology with this methodology will be reinforced with more evaluators who should have different degrees of experience in RM.

In order to strengthen the evaluation, three application scenarios were successfully conducted. The first represents a hypothetical real-world scenario, through the creation of an instance of the ontology. This instance is based on the extraction of information present in the approaches to RM used for the implementation of the SRMO and from scientific literature associated with RM. This instance was implemented using the Protégé editor and with the help of the Hermit reasoner, it could be verified that the ontology is consistent. All CQs were also applied in SPARQL which allowed us to verify the concepts and their relationships and to demonstrate that the ontology meets its requirements with respect to the results achieved and to refine it where necessary. The second application scenario was in a real environment, which allowed us to demonstrate the usefulness of the SRMO. The ontology was used to analyse the implementation of strategies to mitigate risks related to COVID-19 and RMS in a higher education institution, where it can be evidenced that ontologies can be of great use to support the activities of verification, validation or improvement of standards, models, methods, processes, etc. [73,115,136]. This is possible because of the type of domain knowledge it integrates and represents. And the third application scenario to support the definition of a specific risk management methodology where we were able to structure the knowledge and its relationships to carry out the definition of each of the processes and their constituent elements. This methodology is part of the definition of a methodological framework for RM which is in the process of being validated.

Therefore, it can be concluded that the SRMO was successfully evaluated and is ready to be used in future studies. Furthermore, we believe that it can help to contribute to improve the existing proposals regarding the formalism used for its construction and the way in which the knowledge of the domain it represents is structured. Therefore, through this proposal it can be demonstrated that it is possible to conceptualise and represent the knowledge associated with RM at different management levels of the organisation. Through the use of different RM approaches widely recognised by the industry and documentation associated with this management practice. This is in order to propose a consistent terminology for this domain and help reduce ambiguities and inconsistencies. Table 18 shows a general mapping of how the SRMO covers the main sources of knowledge used for its construction (ISO 31000, COBIT 2019, PMBOK, CMMI V2.0).

Table 18. General mapping between RM approaches and the SRMO

Approaches to risk management	SRMO		
	RMEO	RCEO	RPMO
ISO 31000:2018			
6.2 Communication and consultation.	X		
6.3 Scope, context and criteria.			
6.3.2 Defining the scope.	X		
6.3.3 External and internal context.		X	
6.3.4 Defining risk criteria.		X	
6.4 Risk assessment.			
6.4.2 Risk identification.			X
6.4.3 Risk analysis.			X
6.4.4 Risk evaluation.			X
6.5 Risk treatment.			
6.5.2 Selection of risk treatment options.			X
6.5.3 Preparing and implementing risk treatment plans.			X
6.6 Monitoring and review.			X
6.7 Recording and reporting.			X
COBIT 2019 Framework			
EDM03 — Ensured Risk Optimization.			
EDM03.01 Evaluate risk management.	X	X	
EDM03.02 Direct risk management.	X		
EDM03.03 Monitor risk management.	X		
APO12 — Managed Risk.			
APO12.01 Collect data.			X
APO12.02 Analyse risk.			X

APO12.03 Maintain a risk profile.				X
APO12.04 Articulate risk.				X
APO12.05 Define a risk management action portfolio.				X
APO12.06 Respond to risk.				X
PMBOK 6th ed				
11.1 plan risk management.			X	
11.2 identify risks.				X
11.3 perform qualitative risk analysis.				X
11.4 perform quantitative risk analysis.				X
11.5 plan risk responses.				X
11.6 implement risk responses.				X
11.7 monitor risks.				X
CMMI V2.0				
RSK 1.1 Identify and record risks or opportunities and keep them updated.				X
RSK 2.1 Analyse identified risks or opportunities.				X
RSK 2.2 Monitor identified risks or opportunities and communicate status to affected stakeholders.				X
RSK 3.1 Identify and use risk or opportunity categories.			X	
RSK 3.2 Define and use parameters for risk or opportunity analysis and handling.			X	X
RSK 3.3 Develop and keep updated a risk or opportunity management strategy.	X		X	
RSK 3.4 Develop and keep updated risk or opportunity management plans.			X	X
RSK 3.5 Manage risks or opportunities by implementing planned risk or opportunity management activities.				X

7 CONCLUSIONS

This paper presents the details of the development and evaluation of a domain ontology for Software Risk Management, called SRMO. One of the main motivations for the development of this ontology was to address the ambiguity in the terminology associated with RM and inconsistencies resulting from the different contexts of application of the existing proposals. This can lead to misinterpretation and so jeopardise the usefulness and benefits of standardised RM practices. In this sense the SRMO can be a valuable contribution to help reduce ambiguity in this domain and improve understanding on the part of each of the stakeholders involved in this type of management. The ontology seeks to provide the integration of a common terminology through the comparison and integration of the concepts that are present in the most widespread and recognised approaches to RM in the industry. Furthermore, it can serve as a useful tool for software engineering and especially for RM in the context of the software life cycle. But we are also aware that our proposal does not solve all the problems in this domain, but rather it serves to lay the foundations for new research that will help to formalise and synthesise the practices of RM.

The SRMO ontology is subdivided into three subontologies which are used to support the establishment of an RMS from an integrated approach at the level of the processes and projects executed in an organisation. The overriding purpose is to allow organisations to establish a more robust RM that could contribute to improving the capability and maturity of the organisation in its conduct of RM practices. The purpose of this management is to create and protect value, improve performance, encourage innovation, and contribute to the achievement of the organisation's objectives at any level, with regards to all its activities and defined functions [71]. The Pipeline framework was applied to assure and verify the quality of the proposed ontology, which was implemented in Protégé and validated by means of competency questions. Furthermore, an example of the instantiation of this ontology for the management of software project risks and two real application scenarios serves to illustrate its potential use.

Although the evaluation enabled us to obtain promising results, this must be completed with the validation of the ontology in software organisations, in order to verify its quality and benefits for the software industry. This would allow us to reinforce the results achieved so far. One possible direction of future research may focus on integrating RM with other domain ontologies that cover other processes in the software life cycle and on using SRMO as a knowledge base for the development of tools to extract and reuse the knowledge generated in the different assets of an organisation. An expected result of this is to help organisations to better automate the activities of the RM process in supporting decision-making and improving the performance of their processes.

ACKNOWLEDGMENTS

Jhon Masso, Francisco Pino and César Pardo would like to thank the Universidad del Cauca, where all three work as assistant professor, full professor, associate professor, respectively, for its contribution to this work.

Professors Félix García and Mario Piattini acknowledge that this work has been funded by: BIZDEVOPS-GLOBAL project (Ministerio de Ciencia, Innovación y Universidades, y Fondo Europeo de Desarrollo Regional FEDER, RTI2018-098309-B-C31); and G3SOFT project (Consejería de Educación, Cultura y Deportes de la Junta de Comunidades de Castilla La Mancha, y Fondo Europeo de Desarrollo Regional FEDER, SBPLY/17/180501/000150).

REFERENCES

[1] Vivek Agrawal. 2016. Towards the Ontology of ISO/IEC 27005: 2011 Risk Management Standard. In *HAISA*.

[2] M Ahmed, A Anjomshoaa, T M Nguyen, and A M Tjoa. 2007. Towards an Ontology-based Risk Assessment in Collaborative Environment Using the SemanticLIFE. In *The Second International Conference on Availability, Reliability and Security (ARES'07)*, 400–407. DOI:https://doi.org/10.1109/ARES.2007.152

[3] Silvia Ansaldi, Marina Monti, Patrizia Agnello, and Franca Giannini. 2012. An Ontology for the Identification of the most Appropriate Risk Management Methodology. In *On the Move to Meaningful Internet Systems: OTM 2012 Workshops*, Springer Berlin Heidelberg, Berlin, Heidelberg, 444–453.

[4] AS/NZS. 2004. *AS/NZS 4360: 2004: risk management*. Standards Australia; Standards New Zealand Sydney.

[5] AXELOS. 2017. *Managing Successful Projects with PRINCE2®* (Sixth edit ed.). AXELOS. Retrieved from https://bit.ly/1buzMiJ

[6] Judson Bandeira, Ig Ibert Bittencourt, Patrícia Espinheira, and Seiji Isotani. 2016. FOCA: A Methodology for Ontology Evaluation. *ArXiv* abs/1612.0, (2016).

[7] Béatrix Barafort, Antoni-Lluís Mesquida, and Antonia Mas. 2017. Integrating risk management in IT settings from ISO standards and management systems perspectives. *Comput. Stand. Interfaces* 54, (2017), 176–185. DOI:https://doi.org/https://doi.org/10.1016/j.csi.2016.11.010

[8] Béatrix Barafort, Antoni-Lluís Mesquida, and Antònia Mas. 2018. Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context. *Comput. Stand. Interfaces* 60, (2018), 57–66. DOI:https://doi.org/https://doi.org/10.1016/j.csi.2018.04.010

[9] Béatrix Barafort, Antoni-Lluís Mesquida, and Antònia Mas. 2019. ISO 31000-based integrated risk management process assessment model for IT organizations. *J. Softw. Evol. Process* 31, 1 (2019), e1984. DOI:https://doi.org/10.1002/smr.1984

[10] Manuel Bertoa, Antonio Vallecillo, and Felix Garcia. 2006. An Ontology for Software Measurement. In *Ontologies for Software Engineering and Software Technology*. Springer-Verlag Berlin Heidelberg, 175–196. DOI:https://doi.org/10.1007/3-540-34518-3_6

[11] Sinéad Boyce and Claus Pahl. 2007. Developing Domain Ontologies for Course Content. *J. Educ. Technol. Soc.* 10, (2007), 275–288.

[12] Mike Brownsword. 2010. A Formalised Approach to the Management of Risk: A Conceptual Framework and Ontology. *Int. J. Knowl. Syst. Sci.* 1, 4 (October 2010), 1–21. DOI:https://doi.org/10.4018/jkss.2010100101

[13] BSI. 2016. *IT-Grundschutz-Katalog*. Retrieved from https://bit.ly/3sMAQX7

[14] Marvin Carr, Suresh Konda, Ira Monarch, Clay Walker, and F. Carol Ulrich. 1993. *Taxonomy-Based Risk Identification. CMU/SEI-93-TR-006.* Pittsburgh, Pennsylvania. Retrieved from https://bit.ly/3vhfse9

[15] Syrine Chaouch, Asma Mejri, and Sonia Ayachi Ghannouchi. 2019. A framework for risk management in Scrum development process. *Procedia Comput. Sci.* 164, (2019), 187–192. DOI:https://doi.org/https://doi.org/10.1016/j.procs.2019.12.171

[16] Michael Christel and Kyo Kang. 1996. *Software Risk Management*. Pittsburgh, PA. Retrieved from https://bit.ly/3EHkIgM

[17] CMMI Institute. 2018. *CMMI Model V2.0*. Retrieved from https://bit.ly/2QlAFFa

[18] CMMI Institute. 2018. *CMMI V2.0 Adoption and Transition Guidance (Version 2.1)*. Retrieved from https://bit.ly/3aAJ6TP

[19] Calero Coral, Ruiz Francisco, and Piattini Mario. 2006. *Ontologies for Software Engineering and Software Technology*. Springer-Verlag, Berlin, Heidelberg.

[20] David Hillson. 2006. Integrated Risk Management As A Framework For Organisational Success. In *PMI Global Congress proceedings*, Project Management Institute, North America, Seattle, WA. Newtown Square, PA, 1–6. Retrieved from bit.ly/3gBw2RV

[21] Susanne Durst and Helio Aisenberg Ferenhof. 2016. Knowledge Risk Management in Turbulent Times BT - Competitive Strategies for Small and Medium Enterprises: Increasing Crisis Resilience, Agility and Innovation in Turbulent Times. In Klaus North and Gregorio Varvakis (eds.). Springer International Publishing, Cham, 195–209. DOI:https://doi.org/10.1007/978-3-319-27303-7_13

[22] Susanne Durst, Christoph Hinteregger, and Malgorzata Zieba. 2019. The linkage between knowledge risk management and organizational performance. *J. Bus. Res.* 105, (2019), 1–10. DOI:https://doi.org/https://doi.org/10.1016/j.jbusres.2019.08.002

[23] Eclipse Foundation. 2018. Eclipse Process Framework Project. Retrieved from https://bit.ly/3kw1GSA

[24] Abioye Elizabeth, Oluwasefunmi Arogundade, Sanjay Misra, Adio Akinwale, and John Adeniran. 2020. Toward ontology-based risk management framework for software projects: An empirical study. *J. Softw. Evol. Process* 32, (June 2020). DOI:https://doi.org/10.1002/smr.2269

[25] ENISA. 2006. *Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools*. Retrieved from

https://bit.ly/2RVp8wp

[26] Cath Everett. 2011. A risky business: ISO 31000 and 27005 unwrapped. *Comput. Fraud Secur.* 2011, 2 (2011), 5–7. DOI:https://doi.org/https://doi.org/10.1016/S1361-3723(11)70015-X

[27] Ricardo A Falbo, Fabiano B Ruy, Gleidson Bertollo, and Denise F Togneri. 2004. Learning How to Manage Risks Using Organizational Knowledge. In *Advances in Learning Software Organizations*, Springer Berlin Heidelberg, Berlin, Heidelberg, 7–18.

[28] Ricardo de Almeida Falbo and Gleidson Bertollo. 2009. A software process ontology as a common vocabulary about software processes. *Int. J. Bus. Process Integr. Manag.* 4, 4 (2009), 239–250. DOI:https://doi.org/10.1504/IJBPIM.2009.032281

[29] Ricardo de Almeida Falbo, Giancarlo Guizzardi, and Katia Cristina Duarte. 2002. An Ontological Approach to Domain Engineering. In *Proceedings of the 14th International Conference on Software Engineering and Knowledge Engineering* (SEKE '02), Association for Computing Machinery, New York, NY, USA, 351–358. DOI:https://doi.org/10.1145/568760.568822

[30] Ricardo Falbo, Crediné Menezes, and A Rocha. 1998. Using Ontologies to Improve Knowledge Integration in Software Engineering Environments. (January 1998).

[31] Dieter Fensel. 2003. *Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce* (2nd ed.). Springer-Verlag, Berlin, Heidelberg.

[32] Mariano Fernández-López, Asunción Gómez-Pérez, and Natalia Juristo. 1997. Methontology: from ontological art towards ontological engineering. (1997).

[33] Silvia Ferrari and Francisco Cribari-Neto. 2004. Beta Regression for Modelling Rates and Proportions. *J. Appl. Stat.* 31, 7 (August 2004), 799–815. DOI:https://doi.org/10.1080/0266476042000214501

[34] Hans-Georg Fill. 2012. An Approach for Analyzing the Effects of Risks on Business Processes Using Semantic Annotations. In *European Conference on Information Systems, ECIS*, ESADE / AIS, Barcelona. Retrieved from https://bit.ly/3dNT6uV

[35] Félix García, Manuel F Bertoa, Coral Calero, Antonio Vallecillo, Francisco Ruíz, Mario Piattini, and Marcela Genero. 2006. Towards a consistent terminology for software measurement. *Inf. Softw. Technol.* 48, 8 (2006), 631–644. DOI:https://doi.org/https://doi.org/10.1016/j.infsof.2005.07.001

[36] Cédric Gaspoz, Ulysse Rosselet, Mathias Rossi, and Mélanie Thomet. 2019. Ontology Driven Feedforward Risk Management. In *New Knowledge in Information Systems and Technologies*, Springer International Publishing, Cham, 253–261.

[37] M Goman. 2019. Current State of IT Risk Analysis in Management Frameworks: Is It Enough? In *2019 60th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, 1–5. DOI:https://doi.org/10.1109/ITMS47855.2019.8940653

[38] J Gomes and M Romão. 2016. Improving Project Success: A Case Study Using Benefits and Project Management. In *Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016*, Elsevier B.V., ISEG- Lisbon School of Economics and Management, Universidade de Lisboa, Lisboa, Portugal, 489–497. DOI:https://doi.org/10.1016/j.procs.2016.09.187

[39] Asunción Gómez-Pérez. 2004. Ontology Evaluation. In *Handbook on Ontologies*, Steffen Staab and Rudi Studer (eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 251–273. DOI:https://doi.org/10.1007/978-3-540-24750-0_13

[40] Asunción Gómez-Pérez, Mariano Fernández-López, Oscar Corcho, and A Gomez-Perez. 2004. *Ontological Engeenering with examples from the areas of Knowledge Management, e-Commerce and the Semantic Web* (First Edit ed.). Springer-Verlag, Berlin, Heidelberg. DOI:https://doi.org/10.1007/b97353

[41] Thomas R Gruber. 1995. Toward principles for the design of ontologies used for knowledge sharing? *Int. J. Hum. Comput. Stud.* 43, 5 (1995), 907–928. DOI:https://doi.org/https://doi.org/10.1006/ijhc.1995.1081

[42] Michael Grüninger and Mark S Fox. 1995. The Role of Competency Questions in Enterprise Engineering BT - Benchmarking — Theory and Practice. In Asbjørn Rolstadås (ed.). Springer US, Boston, MA, 22–31. DOI:https://doi.org/10.1007/978-0-387-34847-6_3

[43] N Guarino. 1998. *Formal Ontology in Information Systems: Proceedings of the 1st International Conference June 6-8, 1998, Trento, Italy* (1st ed.). IOS Press, NLD.

[44] Nicola Guarino, Birger Andersson, Paul Johannesson, and B Livieri. 2016. Towards an ontology of value ascription. In *Formal Ontology in Information Systems: Proceedings of the 9th International Conference (FOIS 2016)*, 331.

[45] Chao Peng Guo and Baptista Nunes Miguel. 2009. Identification and assessment of risks associated with ERP post-implementation in China. *J. Enterp. Inf. Manag.* 22, 5 (January 2009), 587–614. DOI:https://doi.org/10.1108/17410390910993554

[46] Chao Peng Guo and Baptista Nunes Miguel. 2009. Surfacing ERP exploitation risks through a risk ontology. *Ind. Manag. & Data Syst.* 109, 7 (January 2009), 926–942. DOI:https://doi.org/10.1108/02635570910982283

[47] F Hayat, A U Rehman, K S Arif, K Wahab, and M Abbas. 2019. The Influence of Agile Methodology (Scrum) on Software Project Management. In *2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 145–149. DOI:https://doi.org/10.1109/SNPD.2019.8935813

[48] G van Heijst, A.Th. Schreiber, and B J Wielinga. 1997. Using explicit ontologies in KBS development. *Int. J. Hum. Comput. Stud.* 46, 2 (1997), 183–292. DOI:https://doi.org/https://doi.org/10.1006/ijhc.1996.0090

[49] Ning Huang and ShiHan Diao. 2008. Ontology-based enterprise knowledge integration. *Robot. Comput. Integr. Manuf.* 24, 4 (2008), 562–571. DOI:https://doi.org/https://doi.org/10.1016/j.rcim.2007.07.007

[50] Juhani Iivari, Rudy Hirschheim, and Heinz K Klein. 1998. A Paradigmatic Analysis Contrasting Information Systems Development Approaches and Methodologies. *Inf. Syst. Res.* 9, 2 (June 1998), 164–193. DOI:https://doi.org/10.1287/isre.9.2.164

[51] IRM. 2002. *A Risk Management Standard*. London. Retrieved from https://bit.ly/3v9WVjQ

[52] ISACA. 2013. *COBIT 5 for Risk*. ISACA, Rolling Meadows, Illinois EE.UU. Retrieved from https://bit.ly/3aBCqEX

[53] ISACA. 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, Illinois EE.UU. Retrieved from https://bit.ly/3aCIaOD

[54] ISACA. 2012. *COBIT 5 Enabling Processes*. ISACA, Rolling Meadows, Illinois EE.UU. Retrieved from https://bit.ly/3ngJZpH

[55] ISACA. 2018. *COBIT 2019 Framework: Introduction and Methodology*. Schaumburg, Illinois USA. Retrieved from https://bit.ly/2QkaWNj

[56] ISACA. 2018. *COBIT 2019 Framework: Governance and Management Objectives*. ISACA, Schaumburg, Illinois USA. Retrieved from https://bit.ly/2S1BnYz

[57] ISACA. 2020. *Risk IT Framework, 2nd Edition* (2nd ed.). ISACA, Schaumburg, Illinois USA. Retrieved from https://bit.ly/3ez23HQ

[58] ISO. 2007. *ISO GUIDE 73: Risk management — Vocabulary — Guidelines for use in standards*. International Organization for Standardization;International Electrotechnical Commission, Geneva, Switzerland.

[59] ISO. 2009. *ISO 31000:2009 Risk management — Principles and guidelines*. Geneva, Switzerlan. Retrieved from https://bit.ly/3AzqCOC

[60] ISO. 2011. *ISO/IEC 27005: Information technology - Security techniques - Information security risk management*. Geneva, Switzerlan. Retrieved from https://bit.ly/39u7BkF

[61] ISO. 2013. *ISO/IEC 27001:2013. Information Security Management System (ISMS) requirements. Technical report*. Retrieved from https://bit.ly/3xlbS4q

[62] ISO. 2014. *ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Geneva, Switzerlan. Retrieved from https://bit.ly/3tYSglv

[63] ISO. 2014. *ISO 55000: Asset management — Overview, principles and terminology*. Geneva, Switzerland. Retrieved from https://bit.ly/3sSuFAB

[64] ISO. 2015. *ISO/IEC/IEEE 15288: Systems and software engineering — System life cycle processes*. Geneva, Switzerland. Retrieved from https://bit.ly/3erT771

[65] ISO. 2015. *ISO 9001: Quality management systems — Requirements*. Geneva, Switzerland. Retrieved from https://bit.ly/3eodemq

[66] ISO. 2017. *ISO/IEC/IEEE 15939: Systems and software engineering — Measurement process*. Geneva, Switzerland. Retrieved from https://bit.ly/3xlRMaw

[67] ISO. 2019. *IEC 31010 Risk management - Risk assessment techniques*. Geneva, Switzerland. Retrieved from https://bit.ly/3u15FbK

[68] ISO. 2021. *ISO/IEC 16085: Systems and software engineering — Life cycle processes — Risk management*. Geneva, Switzerland. Retrieved from https://bit.ly/3vefe7A

[69] ISO/IEC/IEEE 12207:2017. 2017. *Systems and software engineering -- Software life cycle processes*. International Organization for Standardization, International Electrotechnical Commission and Institute of Electrical and Electronics Engineers. Retrieved from https://bit.ly/3tOc76b

[70] ISO/IEC 31010:2009. 2009. *Risk management - Risk assessment techniques*. International Organization for Standardization and International Electrotechnical Commission.

[71] ISO 31000:2018. 2018. *Risk management -- Guidelines*. International Organization for Standardization. Retrieved from https://bit.ly/3ayP1ZG

[72] ISO Guide 73:2009. 2009. *ISO Guide 73:2009 Risk management -- Vocabulary*. Retrieved from https://bit.ly/3vegTtQ

[73] S Isotani, I Ibert Bittencourt, E Francine Barbosa, D Dermeval, and R Oscar Araujo Paiva. 2015. Ontology Driven Software Engineering: A Review of Challenges and Opportunities. *IEEE Lat. Am. Trans.* 13, 3 (2015), 863–869. DOI:https://doi.org/10.1109/TLA.2015.7069116

[74] Anant Joshi, Laury Bollen, Harold Hassink, Steven De Haes, and Wim Van Grembergen. 2018. Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. *Inf. Manag.* 55, 3 (2018), 368–380. DOI:https://doi.org/https://doi.org/10.1016/j.im.2017.09.003

[75] Brandy E King and Kathy B T - Finding the Concept Reinold Not Just the Word (Eds.). 2008. *Finding the Concept, Not Just the Word A Librarian's Guide to Ontologies and Semantics*. Chandos Publishing Oxford - England. Retrieved from shorturl.at/duF59

[76] Herfried Kohl. 2020. Generic Standards for Management Systems: An Overview BT - Standards for Management Systems: A Comprehensive Guide to Content, Implementation Tools, and Certification Schemes. In Herfried Kohl (ed.). Springer International Publishing, Cham, 19–249. DOI:https://doi.org/10.1007/978-3-030-35832-7_2

[77] Sandra Lovrencic and Mirko Cubrilo. 2008. Ontology Evaluation - Comprising Verification and Validation. In *In Central European Conference on Information and Intelligent Systems (CECIIS-2008)*, Zagreb, Croatia, 7.

[78] I Lykourentzou, A Kalliakmanis, T Latour, E Kapetanios, K Papadaki, Y Djaghloul, and I Charalabis. 2011. Ontology-based operational risk management. In *13th IEEE International Conference on Commerce and Enterprise Computing, CEC 2011*, Centre de Recherche Public Henri Tudor, Luxembourg, Luxembourg, 153–160. DOI:https://doi.org/10.1109/CEC.2011.18

[79] Ruane Fernandes de Magalhães, Ângela de Moura Ferreira Danilevicz, and Joseph Palazzo. 2019. Managing trade-offs in complex scenarios: A decision-making tool for sustainability projects. *J. Clean. Prod.* 212, (2019), 447–460. DOI:https://doi.org/https://doi.org/10.1016/j.jclepro.2018.12.023

[80] Jhon Masso and César Pardo. 2015. Toward an Ontology for Software Development Governance in Smes. *Rev. Publicaciones e Investig.* 9, (October 2015), 107–119. DOI:https://doi.org/10.22490/25394088.1437

[81] Jhon Masso, Francisco J Pino, César Pardo, Félix García, and Mario Piattini. 2020. Risk management in the software life cycle: A systematic literature review. *Comput. Stand. Interfaces* 71, (2020), 103431. DOI:https://doi.org/https://doi.org/10.1016/j.csi.2020.103431

[82] Melinda McDaniel and Veda C Storey. 2019. Evaluating Domain Ontologies: Clarification, Classification, and Challenges. *ACM Comput. Surv.* 52, 4 (September 2019). DOI:https://doi.org/10.1145/3329124

[83] Jr. Menezes J., C Gusmão, and H Moura. 2019. Risk factors in software development projects: a systematic literature review. *Softw. Qual. J.* 27, 3

(2019), 1149–1174. DOI:https://doi.org/10.1007/s11219-018-9427-5

[84] Lisa Meulbroek. 2002. The Promise and Challenge of Integrated Risk Management. *Risk Manag. Insur. Rev.* 5, 1 (September 2002), 55–66. DOI:https://doi.org/10.1111/1098-1616.00006

[85] Lisa K. Meulbroek. 2002. Integrated Risk Management for the Firm: A Senior Manager's Guide. *SSRN Electron. J.* (2002). DOI:https://doi.org/10.2139/ssrn.301331

[86] Camilo Micán, Gabriela Fernandes, Madalena Araújo, and Enrique Ares. 2019. Operational risk categorization in project-based organizations: A theoretical perspective from a project portfolio risk lens. *Procedia Manuf.* 41, (2019), 771–778. DOI:https://doi.org/https://doi.org/10.1016/j.promfg.2019.09.069

[87] Minciencias. Standard Model of Internal Control (MECI). Retrieved August 9, 2020 from https://bit.ly/3lJFK5O

[88] Maxim Miterev, Mauro Mancini, and Rodney Turner. 2017. Towards a design for the project-based organization. *Int. J. Proj. Manag.* 35, 3 (2017), 479–491. DOI:https://doi.org/https://doi.org/10.1016/j.ijproman.2016.12.007

[89] Hayley Mizen, Catherine Dolbear, and Glen Hart. 2005. Ontology Ontogeny: Understanding How an Ontology Is Created and Developed BT - GeoSpatial Semantics. Springer Berlin Heidelberg, Berlin, Heidelberg, 15–29.

[90] Mark A. Musen. 2015. The Protégé Project: A Look Back and a Look Forward. *AI Matters* 1, 4 (2015), 4–12. DOI:https://doi.org/10.1145/2757001.2757003

[91] Giancarlo Nota, Rossella Aiello, and Maria Pia Di Gregorio. 2010. Ontology Based Risk Management BT - Decision Theory and Choices: a Complexity Approach. Springer Milan, Milano, 235–251.

[92] Natalya F. Noy and Deborah L. Mcguinness. 2001. *Ontology Development 101: A Guide to Creating Your First Ontology*. Retrieved from https://stanford.io/3gO7iWT

[93] Jason R C Nurse and Jane E Sinclair. 2009. Supporting the Comparison of Business-Level Security Requirements within Cross-Enterprise Service Development BT - Business Information Systems. Springer Berlin Heidelberg, Berlin, Heidelberg, 61–72.

[94] H Oktaba, F García, M Piattini, F Ruiz, F J Pino, and C Alquicira. 2007. Software Process Improvement: The Competisoft Project. *Computer (Long. Beach. Calif).* 40, 10 (2007), 21–28. DOI:https://doi.org/10.1109/MC.2007.361

[95] Claudinei Oliveira and Edmo Rodovalho. 2019. Application of ISO 31000 standard on tailings dam safety. *Rem Rev. Esc. Minas* 72, (February 2019), 47–54. DOI:https://doi.org/10.1590/0370-44672018720123

[96] OMG. 2008. *Software & Systems Process Engineering Meta-Model Specification V2.0*. Retrieved from https://bit.ly/3sPY5Q1

[97] OMG. 2008. *Software & Systems Process Engineering Metamodel (SPEM 2.0)*. Retrieved from https://bit.ly/2W1zgGz

[98] César Jesús Pardo-Calvache, Félix Oscar García-Rubio, Mario Piattini- Velthuis, Francisco Jose Pino-Correa, and MaríaTeresa Baldassarre. 2014. A reference ontology for harmonizing process- reference models. *Rev. Fac. Ing. Univ. Antioquia* (2014), 29–42. Retrieved from https://bit.ly/32MqZG2

[99] César Pardo, Francisco J Pino, Félix García, Mario Piattini, and Maria Teresa Baldassarre. 2012. An ontology for the harmonization of multiple standards and models. *Comput. Stand. Interfaces* 34, 1 (2012), 48–59. DOI:https://doi.org/https://doi.org/10.1016/j.csi.2011.05.005

[100] Mauro Gonçalves Pinheiro and Mehran Misaghi. 2014. Proposal of a Framework of Lean Governance and Management of Enterprise IT. In *Proceedings of the 16th International Conference on Information Integration and Web-Based Applications & Services* (iiWAS '14), Association for Computing Machinery, New York, NY, USA, 554–558. DOI:https://doi.org/10.1145/2684200.2684367

[101] Benedikt Pittl, Hans-Georg Fill, and Gerald Honegger. 2017. Enabling risk-aware enterprise modeling using semantic annotations and visual rules. In *Twenty-Fifth European Conference on Information Systems (ECIS), Guimarães,Portugal*, ECIS, Guimarães,Portugal.

[102] PMI. 2009. *Practice Standard for Project Risk Management*. Project Management Institute, Inc., Newtown Square, PA USA. Retrieved from https://bit.ly/3tQb9WO

[103] PMI. 2013. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* (Fifth Edit ed.). Project Management Institute Inc, Newton Square, Pennsylvania USA.

[104] PMI. 2017. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* (Sixth Edit ed.). Project Management Institute, Inc., Newtown Square, PA USA. Retrieved from https://bit.ly/2gDuS9V

[105] PMI. 2019. *The Standard for Risk Management in Portfolios, Programs, and Projects*. Project Management Institute, Inc., Newton Square, Pennsylvania USA. Retrieved from https://bit.ly/2QUIlxI

[106] PMI. 2020. *Pulse of the Profession 2020*. Newtown Square, PA USA. Retrieved from https://bit.ly/2QPoIau

[107] A Poth, S Sasabe, A Mas, and A.-L. Mesquida. 2019. Lean and agile software process improvement in traditional and agile environments. *J. Softw. Evol. Process* 31, 1 (2019). DOI:https://doi.org/10.1002/smr.1986

[108] D Proença, J Estevens, R Vieira, and J Borbinha. 2017. Risk Management: A Maturity Model Based on ISO 31000. In *2017 IEEE 19th Conference on Business Informatics (CBI)*, 99–108. DOI:https://doi.org/10.1109/CBI.2017.40

[109] Diogo Proença and José Borbinha. 2018. Formalizing ISO/IEC 15504-5 and SEI CMMI v1.3 – Enabling automatic inference of maturity and capability levels. *Comput. Stand. Interfaces* 60, (2018), 13–25. DOI:https://doi.org/https://doi.org/10.1016/j.csi.2018.04.007

[110] Md.F. Rabbi and K O B Mannan. 2008. A review of software risk management for selection of best tools and techniques. In *9th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2008 in conjunction with 2nd International Workshop on Advanced Internet Technology and Applications, AITA 2008*, Blekinge Institute of Technology, 773–778. DOI:https://doi.org/10.1109/SNPD.2008.127

[111] C. R Rene Robin and G. V. Uma. 2011. Development of educational ontology for software risk analysis. 610–615.

DOI:https://doi.org/10.1145/1947940.1948067

[112] Antonio Rodríguez, Francisco Ortega, and Ramiro Concepción. 2017. An intuitionistic method for the selection of a risk management approach to information technology projects. *Inf. Sci. (Ny).* 375, (2017), 202–218. DOI:https://doi.org/https://doi.org/10.1016/j.ins.2016.09.053

[113] C Rojrattanakorn and W Vatanawood. 2017. Automated Risk Identification of CMMI Project Planning Using Ontology. In *2017 5th Intl Conf on Applied Computing and Information Technology/4th Intl Conf on Computational Science/Intelligence and Applied Informatics/2nd Intl Conf on Big Data, Cloud Computing, Data Science (ACIT-CSII-BCD)*, 19–24. DOI:https://doi.org/10.1109/ACIT-CSII-BCD.2017.26

[114] Catherine Roussey, Francois Pinet, Myoung Ah Kang, and Oscar Corcho. 2011. An Introduction to Ontologies and Ontology Engineering BT - Ontologies in Urban Development Projects. In Gilles Falquet, Claudine Métral, Jacques Teller and Christopher Tweed (eds.). Springer London, London, 9–38. DOI:https://doi.org/10.1007/978-0-85729-724-2_2

[115] Francisco Ruiz and José Hilera. 2006. Using Ontologies in Software Engineering and Technology. In *Ontologies for Software Engineering and Software Technology*. Springer-Verlag Berlin Heidelberg, 49–102. DOI:https://doi.org/10.1007/3-540-34518-3_2

[116] FRANCISCO RUIZ, AURORA VIZCAÍNO, MARIO PIATTINI, and FELIX GARCÍA. 2004. AN ONTOLOGY FOR THE MANAGEMENT OF SOFTWARE MAINTENANCE PROJECTS. *Int. J. Softw. Eng. Knowl. Eng.* 14, 03 (June 2004), 323–349. DOI:https://doi.org/10.1142/S0218194004001646

[117] Tiago Prince Sales, Fernanda Baião, Giancarlo Guizzardi, João Paulo A Almeida, Nicola Guarino, and John Mylopoulos. 2018. The Common Ontology of Value and Risk. In *Conceptual Modeling*, Springer International Publishing, Cham, 121–135.

[118] Tiago Prince Sales, Nicola Guarino, Giancarlo Guizzardi, and John Mylopoulos. 2017. An ontological analysis of value propositions. In *2017 IEEE 21st International Enterprise Distributed Object Computing Conference (EDOC)*, 184–193.

[119] D Sarantis and D Askounis. 2009. A project management ontology as a reference for e-Government projects. In *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*, 1–8. DOI:https://doi.org/10.1109/ICITST.2009.5402526

[120] SEI. 2010. *CMMI for Development, Version 1.3 - CMU/SEI-2010-TR -033*. Pittsburgh, Pennsylvania EE.UU. DOI:https://doi.org/10.1184/R1/6572342.v1

[121] Gabriel Henrique Silva Rampini, Harmi Takia, and Fernando Tobal Berssaneti. 2019. Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes. *Procedia Manuf.* 39, (2019), 894–903. DOI:https://doi.org/https://doi.org/10.1016/j.promfg.2020.01.400

[122] Regine Slagmulder and Bart Devoldere. 2018. Transforming under deep uncertainty: A strategic perspective on risk management. *Bus. Horiz.* 61, 5 (2018), 733–743. DOI:https://doi.org/https://doi.org/10.1016/j.bushor.2018.05.001

[123] G Soydan and Mieczyslaw M Kokar. 2006. An OWL Ontology for Representing the CMMI-SW Model. In *Workshop on Semantic Web Enabled Software Engineering (SWESE)*, Athens, GA, U.S.A. Retrieved from shorturl.at/uDR23

[124] Rudi Studer, V.Richard Benjamins, and Dieter Fensel. 1998. Knowledge engineering: Principles and methods. *Data Knowl. Eng.* 25, 1 (1998), 161–197. DOI:https://doi.org/https://doi.org/10.1016/S0169-023X(97)00056-6

[125] Jarot S Suroso and Muhammad A Fakhrozi. 2018. Assessment of Information System Risk Management with Octave Allegro at Education Institution. *Procedia Comput. Sci.* 135, (2018), 202–213. DOI:https://doi.org/https://doi.org/10.1016/j.procs.2018.08.167

[126] C Tautz and Christiane Gresse von Wangenheim. 1998. *REFSENO: A representation formalism for software engineering ontologies - IESE-Report No. 015.98/E*. Kaiserslautern - Germany. Retrieved from https://bit.ly/3sNeOnc

[127] Treasury Board of Canada Secretariat. 2016. Guide to Integrated Risk Management. *Government of Canada*. Retrieved April 15, 2020 from https://bit.ly/3gIqZPs

[128] Mike Uschold and Michael Gruninger. 1996. Ontologies: principles, methods and applications. *Knowl. Eng. Rev.* 11, 2 (1996), 93–136. DOI:https://doi.org/DOI: 10.1017/S0269888900007797

[129] Denny Vrandečić. 2010. Ontology Evaluation. Karlsruher Instituts für Technologie (KIT). Retrieved from https://bit.ly/3dLt2k0

[130] W3C. 2012. *OWL 2 Web Ontology Language Document Overview*. Retrieved from https://bit.ly/3tO2ioH

[131] W3C. 2013. *SPARQL 1.1 Query Language*. Retrieved from https://bit.ly/3tUo6PG

[132] Juliano Araujo Wickboldt, Luís Armando Bianchin, Roben Castagna Lunardi, Lisandro Zambenedetti Granville, Luciano Paschoal Gaspary, and Claudio Bartolini. 2011. A framework for risk assessment based on analysis of historical information of workflow execution in IT systems. *Comput. Networks* 55, 13 (2011), 2954–2975. DOI:https://doi.org/https://doi.org/10.1016/j.comnet.2011.05.025

[133] Sari Agustin Wulandari, Anggi Permata Dewi, M Rizki Pohan, Dana Indra Sensuse, M Mishbah, and Syamsudin. 2019. Risk Assessment and Recommendation Strategy Based on COBIT 5 for Risk: Case Study SIKN JIKN Helpdesk Service. *Procedia Comput. Sci.* 161, (2019), 168–177. DOI:https://doi.org/https://doi.org/10.1016/j.procs.2019.11.112

[134] Abir Yamami, Souad Ahriz, Khalifa Mansouri, Mohammed Qbadou, and El Illoussamen. 2017. Representing IT Projects Risk Management Best Practices as a Metamodel. *Eng. Technol. Appl. Sci. Res.* 7, (October 2017), 2062.

[135] Abir El Yamami, Khalifa Mansouri, Mohammed Qbadou, Elhossein Illoussamen, Majida Laaziri, and Khaoula Benmoussa. 2018. An Ontological Representation of PMBOK Framework Knowledge Areas. In *Proceedings of the 3rd International Conference on Smart City Applications* (SCA '18), Association for Computing Machinery, New York, NY, USA. DOI:https://doi.org/10.1145/3286606.3286825

[136] Lan Yang, Kathryn Cormican, and Ming Yu. 2019. Ontology-based systems engineering: A state-of-the-art review. *Comput. Ind.* 111, (2019), 148–171. DOI:https://doi.org/https://doi.org/10.1016/j.compind.2019.05.003