On IT Risk Management Ontology using DEMO

Mariana Rosa[1,2], Sérgio Guerreiro[1,2] and Rúben Pereira[3]
[1]*INESC-ID, Rua Alves Redol 9, 1000-029 Lisbon, Portugal*
[2]*Instituto Superior Técnico, University of Lisbon, Av. Rovisco Pais 1, 1049-001 Lisbon, Portugal*
[3]*Instituto Universitário de Lisboa (ISCTE-IUL), Lisbon, Portugal*

Keywords: DEMO, Essential Model, IT RM, Ontology, SLR.

Abstract: Nowadays, organisations use and rely on Information Technology (IT) solutions. However, despite their benefits, IT solutions induct risks. Consequently, organisations implement Risk Management (RM), more specifically Information Technology Risk Management (IT RM), in order to maximize the effectiveness of IT usage while dealing with IT risks. Nevertheless, IT RM's implementation is not easy, since numerous standards and frameworks propose multiple RM processes to deal with IT risks. Moreover, these processes are composed of different activities causing confusion. In the end, organisations are not capable of managing risks successfully due to IT RM's complexity. To overcome IT RM diversity, a Systematic Literature Review (SLR) was conducted. The goal is to identify which are the most essential IT RM activities. The SLR results were then integrated with ISO 31000 and PMBOK standards in the form of an ontology using Design and Engineering Methodology Ontology (DEMO). The contributions of this study are: the aggregate analysis of IT RM activities through the SLR; the identification of reasons and benefits of using DEMO; a description of an IT RM's *essential model* designed as an ontology; and a critical view of the benefits of the ontological model proposed.

1 INTRODUCTION

Organisations depend on Information Technology (IT) to survive in the current market. Despite the benefits of this dependency, it inducts risks that can affect the achievement of corporate goals. To maximize the effectiveness of IT usage and to manage the risks associated with it, organisations implement a specialisation of Risk Management (RM) - Information Technology Risk Management (IT RM) (Ernawati and Nugroho, 2012). RM is defined as "coordinated activities to direct and control an organisation with regard to risk" (ISO, 2018). In IT RM, RM activities are applied to IT so as to manage IT risks, such as security breaches (T. Yaqoob et al., 2019), loss of computer system data, among others (S. A. Torabi, 2016).

If an organisation has the ability to successfully manage risk, it can modify it so that the organisation is more likely to meet its goals. Therefore it is crucial for organisations to perform IT RM (Purdy, 2010). However, organisations face difficulties in implementing IT RM. There are numerous standards, frameworks and related literature that propose different RM processes to deal with IT risks, causing some confusion regarding the concepts/relationships of IT RM. Furthermore, these standards and frameworks have their own limitations, so the research community is continuously proposing new frameworks(S. Islam, 2014). To overcome IT RM's diversity, this research used the Systematic Literature Review (SLR) methodology, based on the guidelines of Kitchenham (2004), in order to answer the following research question: Which are the concepts/relationships of IT RM that should compose an ontology of this process?

Besides this process's diversity, IT RM's domain is complex since it encompasses many processes and concepts. Therefore, a well-defined IT RM ontology that captures IT RM concepts/relations would create a great step forward in simplifying and clarifying IT RM, thus facilitating IT RM's implementation.

By searching for the topic of interest *"risk management" AND "ontology"* in the databases of Web of Science Core Collection, KCI-Korean Journal Database, Russian Science Citation Index, Current Contents Connect and SciELO Citation Index, 73 articles reaching as far back as 2019 (included) were found. This number is considerably low when considering that the *solo* interest topic *"risk management"* results in 55203 articles in the same databases. Moreover, the 73 articles related with ontology are applied to multiple research areas and not as an abstract risk

Rosa, M., Guerreiro, S. and Pereira, R.
On IT Risk Management Ontology using DEMO.
DOI: 10.5220/0010146002580266
In *Proceedings of the 12th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2020) - Volume 2: KEOD*, pages 258-266
ISBN: 978-989-758-474-9

management approach. Therefore, it is hypothesized that an RM ontology is still an open research area and the domain-specific applications are preferred. IT RM is a well-defined domain-specific RM application where many of the frameworks and standards available demand a consensus ontological definition effort.

The main goal of this research is to produce an ontology of IT RM, using as input the results of the SLR conducted. Design and Engineering Methodology Ontology (DEMO) was used to produce the IT RM ontology (J. L. Dietz, 2020).

The structure of this study is as follows. Section 2 provides a brief summary of the SLR methodology applied to gather information and the results achieved. The SLR offers a clear and comprehensive overview regarding IT RM, that was used as a basis for defining an IT RM's ontology. The procedure of producing the ontology and the models that constitute the ontology itself are described and presented in Section 3. Finally, the conclusions and directions for further research are described in Section 4.

2 SYSTEMATIC LITERATURE REVIEW

When we started to study the literature related to IT RM, we found out that this process encompasses several concepts and processes, and that there is some confusion regarding IT RM concepts/relations, more specifically the IT RM activities. Standards such as the International organisation for Standardization (ISO) 31000, Project Management Body of Knowledge (PMBOK), among others, are not consensual regarding IT RM activities. Moreover, the research community is continuously proposing new RM frameworks due to the limitations of such standards.

The goal of performing this SLR is to gather data concerning IT RM activities and their relationships, proposed or not by known standards and frameworks, in order to find out the essential activities of IT RM.

2.1 SLR Process

This work's SLR is based on the guidelines of Kitchenham (2004). The tasks taken to conduct this review are shown in Table 1.

Four electronical repositories were used to obtain information about the IT RM activities: IEEE Xplore Digital Library, ACM, AIS, ScienceDirect.

This review was first based on a search with the chosen keywords in each repository and without any filter, resulting in a total of 4074 articles. Then, five filters were created following this order:

Table 1: Systematic Literature Review main phases.

Planning Systematic Literature Review	Conducting Systematic Literature Review	Reporting the Review
The need for a systematic review: - IT RM is complex and diverse, with no consensus regarding this process activities.	Filters' application and final articles: - 50 articles.	Findings report: - Discussion about gathered data and draw conclusions.
Research question: - Which are the concepts and relationships of IT RM that should compose an ontology of this process?	Data extraction and analysis: - Reading and further analysis of the articles resulted in a final set of 44 articles; - Sample characteristics; - Information extraction regarding IT RM concepts/relations.	
Review protocol: - Search string; - Filters; - Repositories; - Inclusion criterion.		

1. Searching for the keywords in the article's title, or abstract, or in the authors' keywords;
2. Removing duplicate articles in the same repository and between repositories;
3. Removing articles that were not in English, articles that were not published in Journals or Conferences, and articles prior to 2009. Given that IT RM is a topic that has evolved and has been highly studied in the past 10 years, this restricted period guarantees that the set of articles analysed only considers recent publications;
4. Deletion of articles published in lower-ranked publications/journals, which were assessed by using Scimago (https://www.scimagojr.com) and Conference Ranks (http://www.conferenceranks.com/#data). For conferences, only A, B, A1, A2, B1 and B2 ranks of ERA and Qualis rankings were considered. When an article was assessed by both rankings, Qualis prevailed. For journals, only Q1 and Q2 ranks were accepted;
5. Finally, manual assessment of article abstracts and introductions. Only articles covering the implementation of RM to IT risks were selected.

The keywords used to do the research were: *"IT Risk Management" AND ("activities" OR "process" OR "stages" OR "frameworks" OR "standards").*

2.2 Results

After applying the filters, the set was composed of 50 articles, which were subject to further analysis. For each article, the following data was extracted: IT RM activities and, if applicable, which standard or framework proposed those activities. Subsequently, six articles were then removed since these: focused on IT problems after the IT risks occurred; described methods that in future search might integrate IT RM, not yet specifying the activities; made reference to IT risks but not to an IT RM process applied to those.

The final set of articles analysed is composed of 44 articles, forming the basis of the SLR results [1].

During the data extraction, it was observed that there is a big diversity of activities that can integrate IT RM since 74 different activities were identified. When analysing the definitions and purposes of these activities, it was noticed that many activities with different names from different articles had the same meaning, decreasing then the number of different activities identified. Some articles proposed activities into their IT RM based on known standards and frameworks while others suggested new frameworks. In total 23 different standards or frameworks were mentioned on the articles analysed [2].

After identifying the IT RM activities and their relevance, relationships between the most defended activities were established, in order to find out which of them are essential. After this extensive analysis, and taking into account if the IT RM activities are defended by known standards, a set of essential IT RM activities is determined. The SLR results are based on ISO 31000:2009 and PMBOK 5: Communication and consultation; Context Establishment; Risk Identification; Risk Analysis; Risk Response Planning; Monitor and Control Risk; Recording and Reporting.

To be aligned with the latest versions of the standards, we study and establish relationships between ISO 31000:2009 and ISO 31000:2018, and PMBOK 5 and PMBOK 6, in order to check if the activities from the previous versions still match the activities proposed by the latest versions. After analysing, and knowing that the literature covering the latest versions is still scarce, we opt for a process based on the latest version of the standards since these are simply updated versions. For example, ISO 31000:2018 describes activities in a simpler and more concise manner, since it contains less RM jargon and less defined terms, and also expands some activities, but it does not change the basic structure and fundamentals of the activities' purpose and definition.

The final IT RM process is composed of nine activities: Communication and consultation; Scope, context and criteria; Identify Risks; Perform Qualitative Risk Analysis; Perform Quantitative Risk Analysis; Plan Risk Responses; Implement Risk Responses; Monitor Risks; Recording and Reporting. These activities' definitions will be presented in section 3.2.

3 IT RM ONTOLOGY USING DEMO

The SLR performed provides the IT RM activities' definitions based on ISO 31000:2018 and PMBOK 6, plus their relationships, dependencies and who is responsible for what. This information serves as input, as shown in Figure 1, for defining an ontology of IT RM using DEMO. An IT RM's ontology is defined in order to facilitate the implementation of IT RM, by dealing with the complexity of this process.

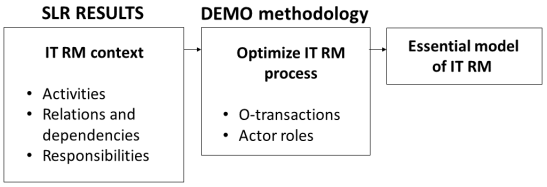

Figure 1: From an SLR to an ontology of IT RM.

3.1 Design and Engineering Methodology Ontology

We chose DEMO because it is a widely accepted methodology that can produce the IT RM's ontology in a systematic way and by simplifying the process. Thus, DEMO facilitates IT RM's implementation and provides explicit and unambiguous concepts for the constructs used in the models (P. Huysmans, 2010).

DEMO comprises a Way of Thinking that consists of Enterprise Engineering (EE) theories, a Way of Modelling containing aspect models, and a Way of Working which supports the making of essential models. This implies that DEMO is mainly about Enterprise Ontology (EO) (J. L. Dietz, 2020).

EO has a strong scientific foundation and provides abstract and high-quality models since it focuses on the organisation's essence regardless all implementation and realisation aspects (Perinforma, 2012). Thus, it facilitates the comprehension of organisations and their operations (Hoogervorst, 2009).

Every organisation is a social system, which means that the system elements are social individuals (actors). An *actor* is a human being that fulfills an *actor role*. The actor role stipulates the authority that the actor may exercise and the responsibility to do so. Commitments are raised in *Coordination acts* (C-acts) and these are always about *Production* facts (P-facts), for example one may request, promise, state, and accept the P-fact *Alice has got the best paper award of LAP'02*. The outcome of performing a C-act is the creation of the corresponding *Coordination fact* (C-fact) (J. L. Dietz, 2020). C-acts/facts always occur in specific patterns of interaction between two actors called transactions, and every transaction is of a particular transaction kind (J. L. Dietz, 2017).

An organisation's actors can be divided into three layers: the O-organisation (O from *Original*), the I-organisation (I from *Informational*), and

the D-organisation (D from *Documental*). The I-organisation supports the O-organisation by remembering, sharing, and deriving facts. The D-organisation supports the I-organisation by storing and fetching documents, or data. An organisation's essence is captured in its O-organisation and the ontological model of an organisation's O-organisation is called its *essential model* (J. L. Dietz, 2020).

In the O-organisation, *Original Production* acts (P-acts) generate original, new P-facts (J. L. Dietz, 2017). A P-act can be the preparation of a cup of tea and the corresponding P-fact is the cup of tea (J. L. Dietz, 2020).

The core elements of an organisation's essential model are the actor roles, C-acts/facts and P-acts/facts. In DEMO Specification Language (DEMOSL)-3, the *essential model* of an organisation consists of four aspect models: Construction Model (CM), Action Model (AM), Process Model (PM) and Fact Model (FM) (J. L. Dietz, 2017).

The CM is the ontological model of an organisation's construction: contains the actor roles, the transaction kinds between actor roles and the information exchanging between actor roles. In DEMOSL-3, the CM is represented in an *Organisation Construction Diagram (OCD)*, a *Transaction Product Table (TPT)*, and a *Bank Contents Table (BCT)* (J. L. Dietz, 2020).

The AM is the ontological model of an organisation's operation, it comprises *action rules* that specify the P/C-acts that must be carried out, along with the P/C-facts that must be assessed. In DEMOSL-3, the AM is represented in *Action Rule Specifications (ARS)* (J. L. Dietz, 2020).

The PM is the ontological model of an organisation's state space and transition space of the Coordination World. Concerning the state space, the PM contains the process step kinds and the applicable existence laws of transaction kinds. Regarding the transition space, the PM comprises the coordination event kinds along with the applicable occurrence laws. In DEMOSL-3, the PM is represented in a *Process Structure Diagram (PSD)* (J. L. Dietz, 2020).

The FM is the ontological model of an organisation's state space and the transition space of the Production World. Concerning the state space, the FM comprises all identified P-fact types. Regarding the transition space, the FM contains the production event types. In DEMOSL-3, the FM is represented in an *Object Fact Diagram (OFD)* (J. L. Dietz, 2020).

3.2 IT RM Activities Analysis

The *essential model* will be based on the IT RM activities' definitions provided by the ISO 31000:2018 and PMBOK 6. The standards were analysed in order to identify the O-organisation transaction kinds (O-transactions) and actor roles, following DEMO.

When analysing the activities' definitions, all realisation aspects of an organisation were ignored. These are I-organisation transaction kinds (I-transactions) and D-organisation transaction kinds (D-transactions). All implementation aspects are disregarded, i.e., the technologies that perform the P-acts and C-acts. Additionally, we abstracted the specific subjects that fulfil the actor roles (Perinforma, 2012).

To identify the O-transactions of IT RM we consider the following criteria: *Original* P-acts/facts encompass manufacturing, transporting, observing, deciding, and judging (J. L. Dietz, 2020).

In the definitions of the activities, their O-, I- and D-transactions are highlighted in italics.

Communication and Consultation, as stated by ISO 31000:2018, is defined as "Communication seeks to *promote awareness and understanding of risk and the means to respond to it*, whereas consultation involves *obtaining feedback and information ...*" (ISO, 2018). Only I-transactions were identified, since these are about sharing and remembering facts.

According to ISO 31000:2018, Scope, context and criteria starts with "The organisation should *define the scope* of its risk management activities", then "The *context of the risk management process should be established ...*", and finally "... *define criteria* to evaluate the significance of risk and to support decision-making processes" (ISO, 2018). Three O-transactions were identified, since they are related to creating something new: *T1 scope defining*, the actor role is A1 scope definer; *T2 context establishing*, the actor role is A2 context establisher; *T3 risk criteria defining*, the actor role is A3 risk criteria definer. These three transactions access organisation data.

Identify Risks, according to PMBOK 6 is about "*identifying individual project risks as well as sources of overall project risk ...*". This standard advises the involvement of experts, so that "*Individual project risks and sources of overall project risk can be identified...*"(PMI, 2017). Two O-transactions were identified, since they are about creating something new: *T4 risks identifying*, the actor role is A4 risks identifier; *T5 individual risks and sources of overall activity risk identifying*, the actor roles are A4 and A5 subject matter proficient. During the process of carrying out T4, the corresponding T5 is initiated, therefore is said that T5 is enclosed in T4, implying that A4 starts T5. In order to identify risks correctly, it is necessary to access information that resulted from T1, T2, T3 and also to access data from the organisation.

According to PMBOK 6, Perform Qualitative

Risk Analysis is about "... *prioritizing individual project risks ...* by *assessing their probability of occurrence* and *impact...*". To successfully assess risks probability of occurrence and their impact, "*Risk data quality may be assessed ...*". Assessing the risks' occurrence probability and impact is subjective, since these assessments are based on perceptions of risk by stakeholders and that is why these are O-transactions. The assessment of risk data quality is also an O-transaction, because a judgement is being made regarding the data available. This activity also "... *identifies a risk owner* for each risk ..." (PMI, 2017). This is an O-transaction, since decisions about who will be responsible for what are being made. In total, five O-transactions were identified: *T6 risks priority assessment*, the actor role is A6 risks analyser; *T7 risks probability of occurrence assessment*, the actor roles are A6 and A7 risks probability of occurrence assessor; *T8 risks impact assessment*, the actor roles are A6 and A8 risks impact assessor; *T9 quality of risks information evaluating*, the actor roles are A7 and A8, and A9 risks information quality evaluator; *T10 risk owner identification*, the actor role is A10 risks owners' identifier. The transactions T7 and T8 are enclosed in T6, and T9 is enclosed in T7 and T8. To perform T6, T7 and T8, the actors need information from T4, and to identify the risk owner, it is necessary to access information that resulted from T1, T2 and also to access data from the organisation.

Perform Quantitative Risk Analysis, as stated by PMBOK 6, is the "... process of *numerically analysing the combined effect of identified individual project risks and other sources of uncertainty...*" (PMI, 2017). This is an I-transaction, since it is about computing, calculating and analysing data.

According to PMBOK 6, Plan Risk Responses is where "... *plans should be developed* by the nominated risk owner" to address risks. Also, "*The strategy or mix of strategies* most likely to be effective *should be selected* for each risk" and where "... *actions are developed* to implement the agreed-upon risk response strategy ...". If necessary, "*A contingency plan...can be developed ...*". "*Secondary risks should also be identified ...*" (PMI, 2017). The previous descriptions correspond to O-transactions, since they are about developing something and deciding: *T11 risk responses planning*, the actor role is A11 risk owner; *T12 risk responses strategies selecting*, the actor roles are A11 and A12 strategies selector; *T13 actions developing*, the actor roles are A11 and A13 actions developer; *T4 risks identifying*, the actor roles are A11 and A4; *T14 contingency plan developing*, the actor roles are A11 and A14 contingency plan developer. The transactions T12, T13 and T14 are all enclosed in T11. To plan risk responses, it is required to take into account the priority of risks, so it is necessary to access T6.

Implement Risk Responses, as stated by PMBOK 6, "Expertise should be considered... to *validate or modify risk responses...and decide how to implement them...*". Also, "*Project documents that may be updated* as a result of carrying out this process", updating outcomes of previous transactions(PMI, 2017). Two O-transactions were identified, where one regards decisions and the other relates to updates that cannot be re-computed, since these depend on new decisions: *T15 risks profile updating*, the actor role is A15 risk responses implementer; *T16 risk responses implementation deciding*, the actor roles are A15 and A16 subject matter expert. The transaction T16 is enclosed in T15. To implement risk responses, it is required to know which are the agreed-upon risk responses, so T15 and T16 actors access T11.

According to PMBOK 6, Monitor Risks relates to "*...monitoring the implementation of agreed-upon risk response plans*, *identifying and analysing new risks*, and *evaluating risk process effectiveness...*" (PMI, 2017). These are all O-transactions, since they are about observing and creating something new: *T17 implementation of risk responses monitoring*, the actor role is A17 risk monitor; *T18 risk management process effectiveness evaluating*, the actor roles are A17 and A18 RM process effectiveness evaluator; *T4 risks identifying*, the actor roles are A17 and A4; *T6 risks priority assessment*, the actor roles are A17 and A6. The transactions T4, T6 and T18 are enclosed in T17. To monitor the implementation of risk responses, it is necessary to access T15.

The last activity is Recording and Reporting, and according to ISO 31000:2018 "The risk management process and its outcomes should be *documented* and *reported...*" (ISO, 2018). These are both I and D-transactions.

3.3 Essential Model of IT RM

Based on the previous analysis, the *essential model* of the IT RM process was produced [3].

The CM was the first model to be produced and it is represented by the TPT, presented in Table 2. It shows the transaction kinds, identified in the subsection 3.2, and corresponding product kinds.

The CM is also represented by the OCD, exhibited in Figure 2. In the OCD the solid lines without a black diamond, between actor roles (squares) and transaction kinds (discs with a red diamond), are called initiator link. These mean that the actors in the actor role (e.g. A6) are an authorised initiator in transactions of

Table 2: Transaction Product Table of IT RM.

Transaction Kind	Product Kind
T1 scope defining	P1 Scope **is** defined
T2 context establishing	P2 Context **is** established
T3 risk criteria defining	P3 Risk criteria **is** defined
T4 risks identifying	P4 Risk **is** identified
T5 individual risks and sources of overall activity risk identifying	P5 Individual risk and source of overall activity risk **is** identified
T6 risks priority assessment	P6 **the** priority **of** Risk **is** assessed
T7 risks probability of occurrence assessment	P7 **the** probability of occurrence **of** Risk **is** assessed
T8 risks impact assessment	P8 **the** impact **of** Risk **is** assessed
T9 quality of risks information evaluating	P9 **the** information's quality **of** Risk **is** evaluated
T10 risks owner identification	P10 Risk Owner **is** identified
T11 risk responses planning	P11 Risk Response **is** planned
T12 risk responses strategies selecting	P12 **the** risk responses strategy **of** Risk Response **is** selected
T13 actions developing	P13 **the** action **of** Risk Response **is** developed
T14 contingency plan developing	P14 **the** contingency plan **of** Risk Response **is** developed
T15 risks profile updating	P15 Risk Profile **is** updated
T16 risk responses implementation deciding	P16 Risk Response Implementation **is** decided
T17 implementation of risk responses monitoring	P17 Risk Response Implementation **is** monitored
T18 risk management process effectiveness evaluating	P18 Risk Management Process Effectiveness **is** reported

the transaction kind (e.g. T8). The solid lines with a black diamond, between actor roles and transaction kinds, represent executor links. These indicate that actors in the actor role (e.g. A8) are an authorised executor in transactions of the transaction kind (e.g. T8). Dashed lines between actor roles and transaction kinds represent information links, the transactions are now conceived as transaction banks. This means that the actors in the connected actor role (e.g. A4) have access to the facts of the transaction bank of the transaction kind (e.g. T1) (J. L. Dietz, 2020).

The next model produced was the PM and is represented by the PSD (Figure 3). It shows the dependencies between the identified processes and in which way a transaction kind is enclosed in another one (Perinforma, 2012).

In the PSD the solid lines represent response links, for example the C-act [+rq] is performed in response to the occurrence of the C-fact (+pm). The dashed lines represent wait links, for example performing the P-act [+ex] must wait for having reached status C-fact (+ac). The discs of the transaction kind shapes are 'stretched' horizontally.

In responding to (T6/rq) A6 performs two acts: one [T6/pm] and [T6/rq]. Next, in response to (T6/pm) A6 initiates T7 and T8. This means that, in order to assess the risks priority, the A6 risks analyser first needs to request for the risks probability of occurrence and the risks impact of occurrence. As soon as the assessments are finished, T6 can be executed. Notice that the brackets "(" and ")" represent C-facts and square brackets "[" and "]" represent C-acts.

In both Figure 2 and 3, the terms "+rq", "+pm", "+ex" and "+ac" mean, respectively request, promise, execute and accept. (J. L. Dietz, 2020).

The next model produced was the FM, represented in an OFD (Figure 4). It specifies which facts are relevant in the Production world (Perinforma, 2012).

In the OFD, the roundangles represent classes, for example RISK. The production event types are represented by red diamonds. For example, the event type "the priority of Risk is assessed" concerns the entity type Risk (or the entity class RISK). Property types are expressed by lines between classes, for instance the property type "the risk profile of Risk is Risk Profile" is a function that maps RISK to RISK PROFILE. The ">" indicates that RISK is the domain of the function and RISK OWNER the range. The class RISK is the core concept of IT RM, and the domain of five product kinds, P4, P6, P7, P8 and P9.

After producing the FM, the BCT (Table 3) was built, completing the CM. It relates all transaction kinds in the CM with the P-fact types in the FM.

Table 3: Bank Contents Table of IT RM.

bank	Independent/dependent facts
T1	SCOPE Scope **is** defined
T2	CONTEXT Context **is** established
T3	RISK CRITERIA Risk criteria **is** defined
T4	RISK Risk **is** identified **the** risk owner **of** Risk **is** Risk Owner **the** risk response **of** Risk **is** Risk Response **the** risk profile of Risk **is** Risk Profile
T5	INDIVIDUAL RISK AND SOURCE OF OVERALL ACTIVITY RISK Individual risk and source **of** overall activity risk **is** identified
T6	**the** priority **of** Risk **is** assessed **the** priority level **of** Risk **is** Float
T7	**the** probability of occurrence **of** Risk **is** assessed **the** risk probability **of** Risk **is** Float
T8	**the** impact **of** Risk **is** assessed **the** risk impact **of** Risk **is** Float
T9	**the** information's quality **of** Risk **is** evaluated
T10	RISK OWNER Risk Owner **is** identified
T11	RISK RESPONSE Risk Response **is** planned **the** risk response implementation **of** Risk Response **is** Risk Response Implementation
T12	**the** risk responses strategy **of** Risk Response **is** selected
T13	**the** action **of** Risk Response **is** developed
T14	**the** contingency plan **of** Risk Response **is** developed
T15	RISK PROFILE Risk Profile **is** updated
T16	RISK RESPONSE IMPLEMENTATION Risk Response Implementation **is** decided
T17	Risk Response Implementation **is** monitored
T18	Risk Management Process Effectiveness **is** reported
AT1	organisation the data of organisation

The AM, consisting of a set of ARS, was the last model to be produced. Action rules are guidelines for actors when dealing with events that they must respond to, and are divided into three parts: the event

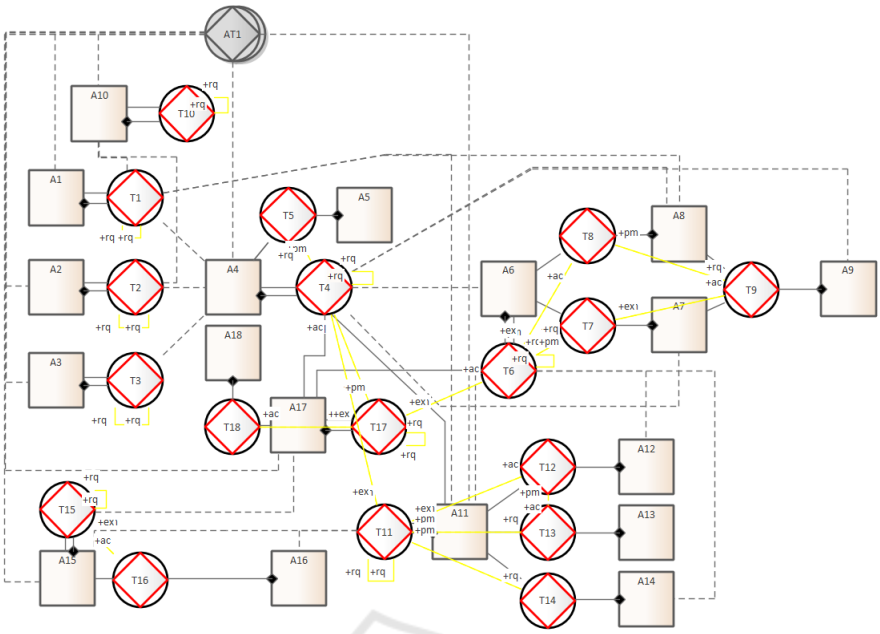

Figure 2: Organisation Construction Diagram of IT RM.

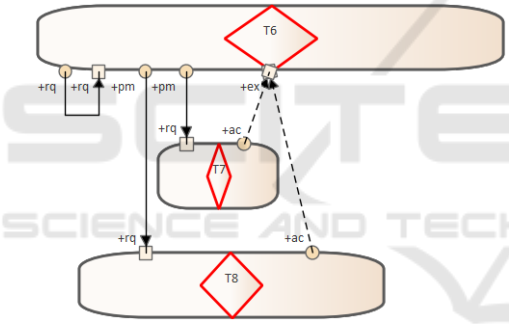

Figure 3: Process Structure Diagram of IT RM, regarding T6. The Plena tool produces a PSD for each transaction. Complete PM at https://rb.gy/9e0lhj.

part, the assess part, and the response part (J. L. Dietz, 2020). One transaction has multiple actions rules, as an example one ARS for T6 is shown in Figure 5.

In Figure 5 the event to respond to is *risks priority assessment* being promised (T6/pm), however the events in the while clause must also have occurred. In this case, the actual settlement of the event must wait until the events in the while-clause (T7/ac and T8/ac) has occurred. In the assess part, we assess the event and check if the actor has the authority to take the role A6 risks analyser. After assessing the conditions, the response part is entered. After checking the intention of promise, if the addressee considers that the intention is valid the addressee will proceed with the event [T6/ex] followed by [T6/st]. The addressee and performer of the promise is the same actor, because T6 is a self-initiating transaction.

The acceptance of *risks impact assessment* (or *risks probability of occurrence assessment*) is the occurrence of the C-fact "accept". A6 only executes *risks priority assessment* after accepting the outcomes of *risks impact assessment* and *risks probability of occurrence assessment*. A6 can only assess the priority of a risk after assessing its probability of occurrence and its impact. So, A6 accepts the result of T7 and T8. The dependency between the execution of T6 with the acceptance of T7 and T8 is shown in Figure 2.

4 DISCUSSION AND CONCLUSIONS

Organisations face difficulties in implementing IT RM, due to its diversity and complexity. When we started studying IT RM, we found out that there is a lack of consensus regarding the IT RM activities. Therefore, an SLR was undertaken to study and analyse RM processes applied to IT risks in order to identify the most essential IT RM activities.

With the main goal of dealing with the complexity of IT RM, an *essential model* of IT RM using DEMO was produced. The IT RM's activities definitions, resulting from the SLR, were used as an input to produce the ontology. By having its roots on EO theory, when producing an essential model using DEMO one acquires an understanding of the organisation's essence that is *comprehensive*, *coherent*, *consistent*, and *concise* (J. L. Dietz, 2020).

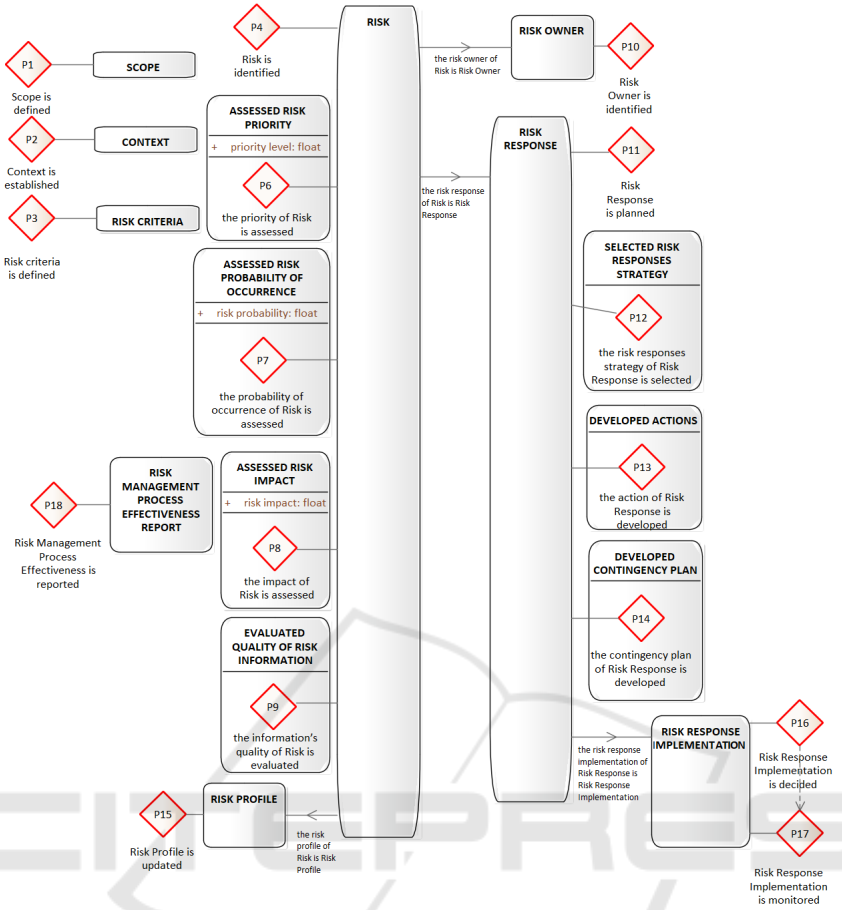

Figure 4: Object Fact Diagram of IT RM.

ARS for T6 (3):

when	risks priority assessment **for** Risk is promised	(T6/pm)
	while risks probability of occurrence assessment **for** Risk is accepted;	(T7/ac)
	risks impact assessment **for** Risk is accepted	(T8/ac)
assess	*justice*: **the** performer **of the** promise **is the** risks analyser	
	the addressee **of the** promise **is the** risks analyser	
sincerity:	<no specific condition>	
truth:	<no specific condition>	
if	*complying with* promise *is considered justifiable*	
then	execute risks priority assessment **for** Risk	[T6/ex]
	state risks priority assessment **for** Risk	[T6/st]
	with **the** addressee **of the** statement **is the** risks analyser	

Figure 5: Action Rule Specification for T6. Complete ARS at https://rb.gy/r3c1a7.

EO provides clear definitions for the constructs used in the aspect models, hence reducing the degrees-of-freedom for the modeler, ensuring that only one correct model can be developed. DEMO also provides clear guidelines, by having a solid theoretical foundation, thus restricting the subjectivity in the modeling process(P. Huysmans, 2010). By being based on the Performance in Social Interaction theory, DEMO models are coherent and consistent.

At first glance, the models produced may be hard to understand by those unfamiliar with the notation. Nevertheless, DEMO models use a limited number of constructs (simplicity) and follow the transaction pattern (completeness and integrity). This limits the number of concepts that someone must learn in order to understand DEMO models(P. Huysmans, 2010).

Additionally, DEMO models do not contain any implementation-related details. Even though this can be considered an advantage regarding flexibility and integration, it is not advised to use DEMO as a standalone for communicating and reenacting IT RM models to other parties. Hence the need to complement it with other techniques and models(P. Huysmans, 2010).

This research contributes to the simplification and clarification of IT RM by facilitating its design, implementation and assessment. Consequently, we increase the chances of successfully implementing an essential IT RM process that is less expensive, either in terms of human and financial resources.

As future work, the IT RM's essential model will

be validated through its application to a real case study, and we will evaluate its completeness. We will then discuss if the IT RM's ontology meets or does not meet the desired objectives, through an analysis and assessment of key performance indicators regarding the outcomes from applying the ontology.

ACKNOWLEDGEMENTS

This work was supported by the European Commission program H2020 under the grant agreement 822404 (project QualiChain) and by national funds through Fundação para a Ciência e a Tecnologia with reference UIDB/50021/2020 (INESC-ID).

REFERENCES

Ernawati, T. and Nugroho, D. (2012). It risk management framework based on iso 31000: 2009. In *2012 International Conference on System Engineering and Technology (ICSET)*, pages 1–8. IEEE.

Hoogervorst, J. A. (2009). *Enterprise governance and enterprise engineering*. Springer Science & Business Media.

ISO (2018). 31000: 2018—risk management—guidelines. 262.

J. L. Dietz, H. B. M. (2020). *Enterprise Ontology: A Human-Centric Approach to Understanding the Essence of Organisation*. Springer Nature.

J. L. Dietz, J. A. H. (2017). Foundations of enterprise engineering.

P. Huysmans, K. Ven, J. V. (2010). Using the demo methodology for modeling open source software development processes. *Information and Software Technology*, 52(6):656–671.

Perinforma, A. P. (2012). The essence of organisation. *South Holland: Sapio Enterprise Engineering*.

PMI, A. (2017). guide to the project management body of knowledge (pmbok guide), 6. ver. *PROJECT MANAGEMENT INSTITUTE (PMI)*.

Purdy, G. (2010). Iso 31000: 2009—setting a new standard for risk management. *Risk Analysis: An International Journal*, 30(6):881–886.

S. A. Torabi, R. Giahi, N. S. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety science*, 89:201–218.

S. Islam, H. Mouratidis, E. R. W. (2014). An empirical study on the implementation and evaluation of a goal-driven software development risk management model. *Information and Software Technology*, 56(2):117–133.

T. Yaqoob, A. Arshad, H. A. et al. (2019). Framework for calculating return on security investment (rosi) for security-oriented organizations. *Future Generation Computer Systems*, 95:754–763.

Notes

[1]Consult the articles' references at https://rb.gy/6fdtkz.

[2]Consult the IT RM activities, and frameworks and standards at https://rb.gy/m24gqg

[3]The Plena tool (https://www.teec2.nl/plenaen/plena-the-tool/) that runs on the Enterprise Architect software was used to produce the *essential model*. The previous sections of this paper refer to DEMOSL-3 because Plena currently supports DEMO version 3.7.