Designing an IT Risk Management Ontology Grounded on Systematic Literature Review

Mariana Rosa
INESC-ID, Portugal
IST, University of Lisbon, Portugal
mariana.rosa@tecnico.ulisboa.pt

Sérgio Guerreiro
INESC-ID, Portugal
IST, University of Lisbon, Portugal
sergio.guerreiro@tecnico.ulisboa.pt

Rúben Pereira
Instituto Universitário de Lisboa
ISCTE-IUL, Lisbon, Portugal
Ruben.Filipe.Pereira@iscte-iul.pt

Abstract

Organizations that operate digital-based services rely heavily on Information Technology (IT). Nonetheless, this IT dependency inducts risks that could impact the achievement of organizations goals and even its own survival. One usual solution is to enforce an IT Risk Management (RM) approach to cope with IT-related risks.

However, due to IT RM complexity and diversity, many organizations are not able to implement it successfully. Therefore, an IT RM ontology capturing the essential of IT RM concepts and its relations constitute a positive step towards the simplification and clarification of IT RM, which by its turn facilitates the IT RM enforcement.

This paper designs an IT RM ontology, using DEMO, that is grounded in a SLR that follows the Kitchenham (2004) guidelines. The objective is to prescribe what key concepts, relationships and processes should be enforced to reduce the IT RM implementation effort when compared with an implementation from scratch.

1. Introduction

With the constant innovation of Information Technology (IT), organizations have realized its benefits to increase the quality, certainty and speed of affairs and the relevance of its use in increasing the organization's efficiency and effectiveness. However, IT also creates risks, so organizations must implement Information Technology Risk Management (IT RM) to secure their information and achievement of their goals.

IT RM consists on the use of Risk Management (RM) activities to IT in order to manage IT risks, such as leakage and alteration of information and the disruption or annihilation of critical IT services [SLR1].

IT RM is essential for organizations' survival. However, organizations face difficulties in implementing this process because several standards, frameworks and related literature propose different RM processes to deal with IT risks. Moreover, organizations have problems in managing IT risks successfully due to the complexity of the IT RM's domain.

The IT RM's domain is complex since it encompasses many processes and concepts. Therefore, a well-defined IT RM ontology that captures IT RM related concepts along with their relationships would constitute a breakthrough in simplifying and clarifying IT RM.

Before defining an ontology, the key concepts/relationships of IT RM must be identified. However, as mentioned above, there is some confusion regarding the RM processes that deal with IT risks, which have been proposed by different well-known standards and frameworks, and consist of different activities. Furthermore, these standards and frameworks have their own limitations, so the research community is continuously proposing new RM frameworks.

One of the goals of this research is to answer the following research question: Which are the key concepts/relationships of RM that should be part of an IT RM ontology? To answer this question, a Systematic Literature Review (SLR) based on the guidelines of Kitchenham (2004) was carried out to review the essential RM activities that are implemented and proposed in the literature to deal with IT risks [1].

After identifying the essential IT RM activities, it is possible to propose an ontology that can be used to capture the essence of IT RM. Design & Engineering Methodology for Organizations (DEMO) was used to produce the IT RM ontology [2].

The structure of this study is as follows. Section 2 explains the SLR methodology used to gather information, as well as the results achieved. Having a clear and comprehensive overview of IT RM provided by the SLR, it was then used as a basis for defining an ontology of this process. The models that constitute the IT RM ontology are presented in Section 3. Finally, the conclusions as well as directions for further research are described in Section 4.

URI: https://hdl.handle.net/10125/71349
978-0-9981331-4-0

2. Methodology

The SLR conducted (depicted in Figure 1) was based on the guidelines of Kitchenham (2004) and consists of three main phases: 1- Planning Systematic Literature Review, 2- Conducting Systematic Literature Review, and 3- Reporting the Review [1].

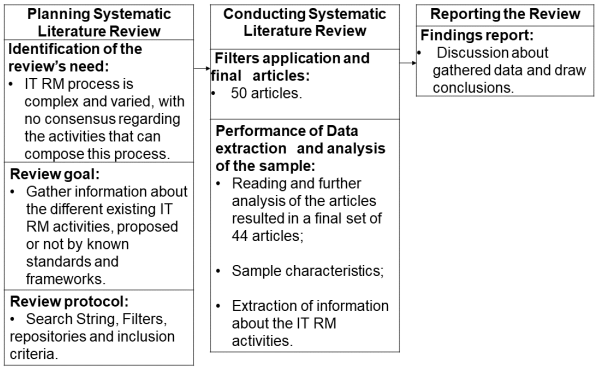

Figure 1. Systematic Literature Review main phases.

2.1. Planning Systematic Literature Review

The planning phase consisted in establishing the goals of this research and the way in which the review will be carried out. As previously mentioned, this SLR is necessary since there is a lack of consensus regarding the activities that compose IT RM.

Before finding literature related to the research question, search terms were defined. The keywords established were: *"IT Risk Management" AND ("activities" OR "process" OR "stages" OR "frameworks" OR "standards").* These were used as strings and the first one was the main search term.

There are some known frameworks and standards that propose IT RM activities, such as International Organisation for Standardization (ISO) 31000, Project Management Body of Knowledge (PMBOK), among others. As such, it was decided to add the "frameworks" and "standards" keywords in order to obtain the IT RM process activities that had a bigger "impact" in the research community by following established frameworks and standards.

To answer the research question, four electronical repositories were chosen to extract data regarding IT RM key concepts/relationships. These include: IEEE Xplore Digital Library, ACM, AIS, and ScienceDirect.

After identifying the keywords and repositories, the searching process begun. First, a search with the keywords in each repository was done without any filter. Then, five filters were created following this order:

1. Search for the keywords in the article's title, or abstract, or article's keywords;
2. Eliminate duplicate articles in the same repository and between repositories;
3. Remove articles that were not in English, articles that were not from journals/scientific magazines and conferences, and articles prior to 2009. The reason for this criterion is because IT RM is a subject that has evolved and has been highly studied in the past 10 years, ensuring that the set analysed only considers recent publications;
4. Remove articles published in lower-ranked publications/journals, ensuring that the articles selected were high-quality peer-reviewed. This process made use of Scimago[1] and Conference Ranks[2]. For conferences, A, B, A1, A2, B1 and B2 ranks of ERA and Qualis rankings were chosen. When an article was assessed by both rankings, Qualis prevailed. For journals, only Q1 and Q2 ranks were acknowledged;
5. Manually asses articles' abstract and introduction. The applied inclusion criterion was the selection of articles that covered the implementation of RM to IT risks, i.e. articles that implicitly or explicitly stated IT RM activities and articles that adopted an IT RM process proposed by known standards and frameworks. Articles that did not meet this condition were excluded.

2.2. Conducting Systematic Literature Review

The articles that resulted from the research made with the keywords were passed through the five filters defined above in each repository. The flow of the filtering process, including the number of articles obtained in each repository and after applying each filter, is shown in Figure 2.

After applying the filters to the articles retrieved from the repositories, 50 articles constituted the final set of articles, and were subject to further analysis. For each article, the following data was extracted: IT RM activities and, if applicable, which standard or framework were those activities from, and other components of IT RM.

Consequently, six articles were eliminated from the final set of articles since these: focused on IT problems prior to the occurrence of IT risks; explained procedures and strategies that in the future search might integrate

[1]Scimago (a journal repository): https://www.scimagojr.com

[2]Conference Ranks (supplies conference ranks): http://www.conferenceranks.com/#data

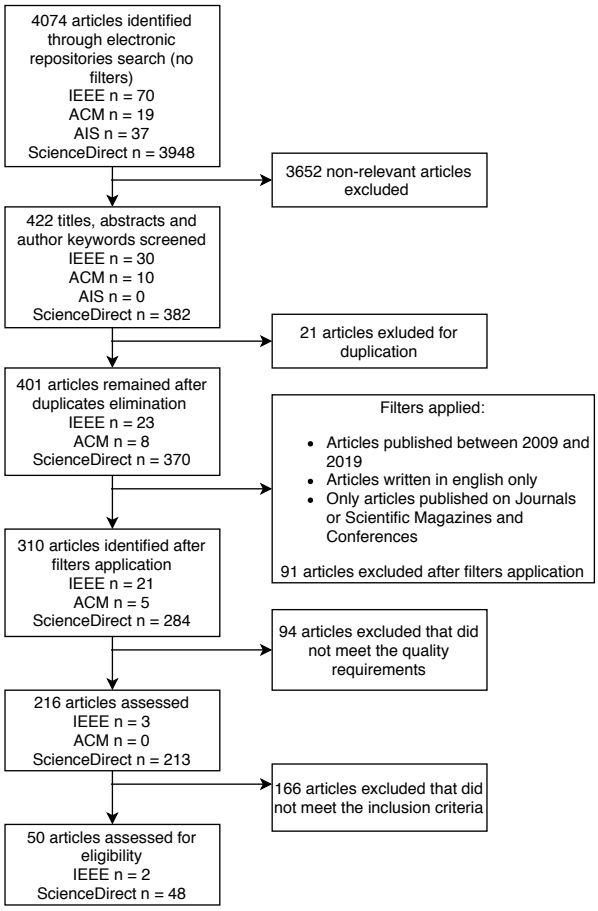

Figure 2. Flow of filtration process.

IT RM, not yet specifying the activities that compose the process; referred to IT risks but did not specify an IT RM process to deal with those.

The final set of articles that was analysed is composed of 44 articles.

2.3. Review results

When analyzing the final set of articles, two key concepts were identified: IT RM activities and frameworks/standards that support those activities.

During the extraction of data from the articles, it was noticed that there is a big diversity of activities that can be part of IT RM since 74 distinct activities were identified (not counting with the activities that are part of other activities). However, when analyzing the definition and purpose of each activity, it was perceived that many IT RM activities with different names from different articles had the same meaning or purpose, resulting in a decrease of the number of distinct activities identified.

In Table 1 the IT RM activities that were mentioned more than once in the final set of articles are presented. The activities that belong to other activities are highlighted in gray. Notice that some articles were not considered in Table 1 since they did not state the activities involved in IT RM, namely articles [SLR2], [SLR3], [SLR4] and [SLR5].

Some articles proposed activities into their IT RM that are supported by known standards and frameworks, such as ISO 31000:2009 and PMBOK 5. These are crucial tools which support organizations in implementing the IT RM process. Nevertheless, these have their own limitations, which leads to the constant creation of new ones. Many articles from the final set proposed new frameworks for IT RM.

The most frequent IT RM activities proposed by the articles of the final set were: Risk Identification; Risk Assessment; Risk Analysis; Risk Treatment, in 9 articles; Risk Response Planning; Context Establishment; Risk Response; RM Planning, in 5 articles; Risk Control; Monitor and Control Risk.

After identifying the IT RM activities and the relevance of each one, the relationships and dependencies between the most popular IT RM activities were established in order to find out which of them are essential. Following this extensive analysis, and taking into account if the IT RM activities were proposed by the latest version of known standards, in this case ISO 31000:2018 and PMBOK 6, a set of the essential IT RM activities was defined.

The literature covering the latest versions of ISO and PMBOK is still scarce, but it was opted for a process composed of activities defended by these versions. The current version of these standards is simply an update of the previous one (ISO 31000:2009 and PMBOK 5). For instance, in ISO 31000:2018, the RM activities' descriptions contain less RM jargon and less defined terms, being more clear and concise. Furthermore, some descriptions were expanded. Therefore, the basic structure and fundamentals of the activities' purpose and definition was not changed.

The first essential activity of IT RM is Communication and Consultation and, according to ISO 31000:2018, this activity is considered to be central to the process. As stated in ISO 31000:2018, it 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 ..."* [3].

Context Establishment (ISO 31000:2009) is equivalent to Scope, context and criteria (ISO 31000:2018). According to ISO 31000:2018, Scope, context and criteria is where *"The organization should define the scope of its risk management activities"*,

Table 1. IT RM activities, that appeared more than once, presented by each SLR bibliographic reference (the black circle represents that the IT RM Activity is referred in the article).

IT RM activity \ Article Reference	[SLR6]	[SLR7]	[SLR8]	[SLR9]	[SLR10]	[SLR11]	[SLR12]	[SLR1]	[SLR13]	[SLR14]	[SLR15]	[SLR16]	[SLR17]	[SLR18]	[SLR19]	[SLR20]	[SLR21]	[SLR22]	[SLR23]	[SLR24]	[SLR25]	[SLR26]	[SLR27]	[SLR28]	[SLR29]	[SLR30]	[SLR31]	[SLR32]	[SLR33]	[SLR34]	[SLR35]	[SLR36]	[SLR37]	[SLR38]	[SLR39]	[SLR40]	[SLR41]	[SLR42]	[SLR43]	[SLR44]	Total
Risk Identification	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●																		22
Risk Assessment (RA)			●	●				●		●			●				●	●	●	●	●			●			●	●		●	●	●			●			●			20
RA - Risk Identification																								●				●				●			●						5
RA - Risk Analysis										●																		●				●			●						5
RA - Risk Evaluation																								●				●				●			●						5
RA - Risk quantification																				●				●																	2
RA - System characterization																														●											1
RA - Threat identification																														●											1
RA – Vulnerability identification																														●											1
RA - Control analysis																														●											1
RA - Likelihood determination																														●											1
RA - Impact analysis																														●											1
RA - Risk determination																														●											1
RA – Control recommendations																														●											1
RA - Results documentation																														●											1
Risk Analysis	●	●			●		●		●		●	●		●	●							●			●	●														12
Risk Analysis - Quantitative																						●																			1
Risk Analysis - Qualitative																						●																			1
Risk Treatment								●			●			●										●		●		●	●			●		●							9
Risk Response Planning		●	●						●				●		●	●						●																			7
Context Establishment											●			●				●	●									●					●									6
Risk Response	●				●																●				●						●		●								6
RM Planning					●							●			●	●						●																			5
Risk Control							●					●			●			●						●																	5
Monitor and Control Risk	●		●										●			●						●																			5
Risk Monitoring		●				●												●	●																						4
Risk Evaluation									●		●			●																								●			4
Scope Establishment		●																							●	●															3
Prioritization of Actions				●															●								●														3
Risk Monitoring and Review											●			●														●													3
Communication and Consultation											●			●														●													3
Effectiveness measurement				●																							●												●	3
Implementation of protection programs				●															●								●														3
Risk Reporting and Recording												●																						●							2
Internal Environment																															●	●								2
Objective Setting																															●	●								2
Event Identification																															●	●								2
Control Activities																															●	●								2
Information and communication																															●	●								2
Monitoring																															●	●								2
Risk Mitigation																																					●	●		2
Threats and vulnerabilities identification																																		●					●	2

"The context of the risk management process should be established from the understanding of the external and internal environment in which the organization operates ...", and where the organization "... should also define criteria to evaluate the significance of risk and to support decision-making processes" [3].

Risk Identification and Risk Analysis definitions were based on PMBOK, since it is one of the most popular standards regarding RM and these two activities were more frequently proposed without being part of Risk Assessment, as proposed by ISO 31000. Identify Risks, according to PMBOK 6, is about "identifying individual project risks as well as sources of overall project risk ...". PMBOK advises the participation of experts in this activity, so that *"Individual project risks and sources of overall project risk can be identified..."*, acquiring a list of those risks and respective sources [4].

PMBOK divides Risk Analysis into two activities: Perform Qualitative Risk Analysis and Perform Quantitative Risk Analysis. Perform Qualitative Risk Analysis, as stated in PMBOK 6, relates to *"... prioritizing individual project risks ... by assessing their probability of occurrence and impact as well as other characteristics"*. To successfully assess risks probability of occurrence and respective impact, *"Risk data quality may be assessed ..."*. Assessing the risks' probability of occurrence and impact is subjective, since this evaluation is based on perceptions of risk by stakeholders. This activity also *"... identifies a risk owner for each risk ..."*. According to PMBOK 6, Perform Quantitative Risk Analysis is the "... process of numerically analysing the combined effect of identified individual project risks and other sources of uncertainty on overall project objectives" [4].

Plan Risk Responses is proposed by both PMBOK 5 and PMBOK 6. 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 required *"A contingency plan (or fallback plan) can be developed ..."*. *"Secondary risks should also be identified ... risks that arise as a direct result of implementing a risk response"* [4].

PMBOK 6 inserted a new activity to its RM process named Implement Risk Responses, where *"Expertise should be considered ... to validate or modify risk responses ... and decide how to implement them ..."*. Additionally, *"Project documents that may be updated as a result of carrying out this process"*, updating results of previous transactions regarding risks [4].

Monitor Risks, as stated by PMBOK 6, is about *"... monitoring the implementation of agreed-upon*

risk response plans, tracking identified risks, identifying and analysing new risks, and evaluating risk process effectiveness ..." [4]. Monitor and Control Risk, one of the most frequent IT RM activities, is equivalent to Monitor Risks plus Implement Risk Responses.

Recording and Reporting and, as stated by ISO 31000:2018, *"The risk management process and its outcomes should be documented and reported through appropriate mechanisms"*. This activity has the purpose of communicating RM activities and results across the organization, providing information for decision-making, improving RM activities and supporting the interaction between stakeholders [3].

Therefore, the final set of essential IT RM activities 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.

3. An IT RM ontology

After identifying the key concepts/relationships of IT RM through an SLR, an ontology of the IT RM process can be defined.

The SLR resulted in an essential IT RM process composed of the most defended activities in the literature related to IT RM. The SLR performed provides the IT RM activities' definitions based on ISO 31000:2018 and PMBOK 6, plus their interrelationships, dependencies and who is responsible for carrying out actions to execute each activity. This information will serve as a basis for defining an ontology of IT RM using DEMO.

DEMO was chosen since it allows the production of an ontology in a systematic way and it offers a remarkable reduction of the process' complexity, therefore facilitating IT RM's comprehension. This methodology is widely accepted in both scientific research and practical appliance.

DEMO comprises a Way of Thinking that consists of Enterprise Engineering (EE) theories, a Way of Modelling composed of four aspect models expressed in the DEMO Specification Language (DEMOSL), and a Way of Working that offers the Organizational Essence Revealing method, that supports the making of essential models. This implies that DEMO is mainly about Enterprise Ontology (EO) [2].

EO supplies a conceptual and high-quality model that focus only on the organization's essence, abstracting from all implementation and realization details [5]. Moreover, one acquires an understanding of the organization's essence that is *coherent* (the four aspect models constitute a logical and truly integral whole), *comprehensive* (all relevant matters are covered), *consistent* (the aspect models are free from discrepancies) and *concise* (no redundant matters are included in the essential model). Such conceptual model is called *ontological model* and it is *essential* [2]. So, an organization's ontological model reduces the difficulty of comprehending the organization itself and its operations [6].

The motto of DEMO is "essence and simplicity", the notion of essence is discussed by some EE theories, being one of them the Performance in Social Interaction (PSI) theory that is about the essence of things.

According to DELTA theory, an EE theory, every organization is a social system, meaning that the system elements are social individuals (actors). PSI theory clarifies the organizations' operation. The operating principle is that actors enter into and comply with commitments towards each other. An *actor* is a subject (human being) filling an *actor role*. The actor role indicates 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 *Fernando has got the best paper award*. The result of performing a C-act is the creation of the corresponding *Coordination fact* (C-fact) [2]. C-acts/facts always occur in specific patterns of interaction between two actors (one in the initiator role and other in the executor role), called transactions. Every transaction (instance) is of a particular transaction kind [7].

The actors in an organization can be split up in three layers: the O-organization (O from *Original*), the I-organization (I from *Informational*), and the D-organization (D from *Documental*). The I-organization supports the O-organization by remembering, sharing, and deriving facts, and the D-organization supports the I-organization by storing and retrieving documents/data. An organization's realization aspect is understood as the devising of the I-organization and the D-organization, given its O-organization. Contrary, abstracting from realization yields the O-organization. So, an organization's essence is captured in its O-organization and the ontological model of an organization's O-organization is its *essential model* [2].

The O-organization is where *original* production occurs. *Original Production* acts (P-acts) bring about original, new, P-facts, and are performed by authorized and responsible actors. P-acts include manufacturing, transporting, observing, devising, deciding, and judging.

For example, a P-act can be baking a cake and the corresponding P-fact is the cake [2].

The core elements of an organization's ontological model are the actor roles, C-acts/facts and P-acts/facts.

In DEMOSL-3, an organization's essential model consists of four aspect models, each taking a certain aspect of the organization: Construction Model, Action Model, Process Model and Fact Model [7].

DEMOSL-3 was chosen as the specification language instead of the latest version DEMOSL-4, since Plena tool will be used to produce the aspect models of IT RM. This tool runs on the Enterprise Architect software and currently supports DEMO version 3.7.

3.1. IT RM Essential Model

Before defining the four aspect models, the IT RM activities' definitions from ISO 31000:2018 and PMBOK 6 were analysed, ignoring all realization and implementation aspects since EO is focused only on the essence of the organization. Therefore, we abstracted from all realization aspects such as I-organization transaction kinds (I-transactions) and D-organization transaction kinds (D-transactions), implementation aspects like technologies that are responsible for executing P-acts and C-acts, and also abstracted from the exact human being that fulfils an actor role [5].

Through this analysis the different O-organization transaction kinds (O-transactions) and actor roles of the IT RM process were identified. After this analysis it is possible to produce the IT RM's essential model. Notice that not all IT RM activities are O-transactions, activities such as Communication and Consultation, Perform Quantitative Risk Analysis and Recording and Reporting are either I-transactions or D-transactions.

In this paper, not every aspect model or components that belong to each model will be presented. Thus, only part of the Construction Model (CM) and the Fact Model (FM) of IT RM's essential model will be presented, giving a simplistic and general view of the process.

The first model to be produced was the CM. It is the ontological model of an organization's construction. Shows the *interaction* structure (i.e. the transaction kinds between actor roles), the corresponding actor roles (that can be internal or external), and the *interstriction* structure (i.e. information exchanging between actor roles). The CM is represented in an *Organization Construction Diagram* (OCD) and a *Transaction Product Table* (TPT) [5, 2].

The TPT, as shown in Table 2, presents identified transaction kinds and their product kinds.

The OCD is presented in Figure 3. The solid lines without a black diamond, between actor roles (squares) and transaction kinds (discs with a red diamond, are *initiator links*. This implies that actors in the actor role (e.g. A11) are an authorised initiator in transactions of the transaction kind (e.g. T12). The solid lines with a black diamond, between actor roles and transaction kinds, represent *executor links*. This means that actors in the actor role (e.g. A12) are an authorised executor in transactions of the transaction kind (e.g. T12). *Information links* are the dashed lines between actor roles and transaction kinds, which are now conceived as transaction banks. This implies that actors in the actor role (e.g. A17) have (reading) access to the facts of the transaction bank of the transaction kind (e.g. T15) [2].

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 enhancing	P15 Risk **is** enhanced
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** evaluated

The transaction bank AT1 contains data regarding the organization: its objectives, time, location, specific inclusions and exclusions, risk assessment tools and techniques, resources, responsibilities and records (such as the lessons learned register), relationships between projects, processes and activities, organization's environmental factors, obligations, among others.

The next model to be defined was the Process Model (PM). It is the ontological model of an organization's state space and transition space of its Coordination World. Regarding the *state space*, for all transaction kinds, between internal actors and between external and internal actors, the PM contains the process step kinds and the applicable existence laws. Concerning the *transition space*, the PM contains the coordination event kinds along with the applicable occurrence laws [5, 2].

Then, the FM was produced. It is the ontological

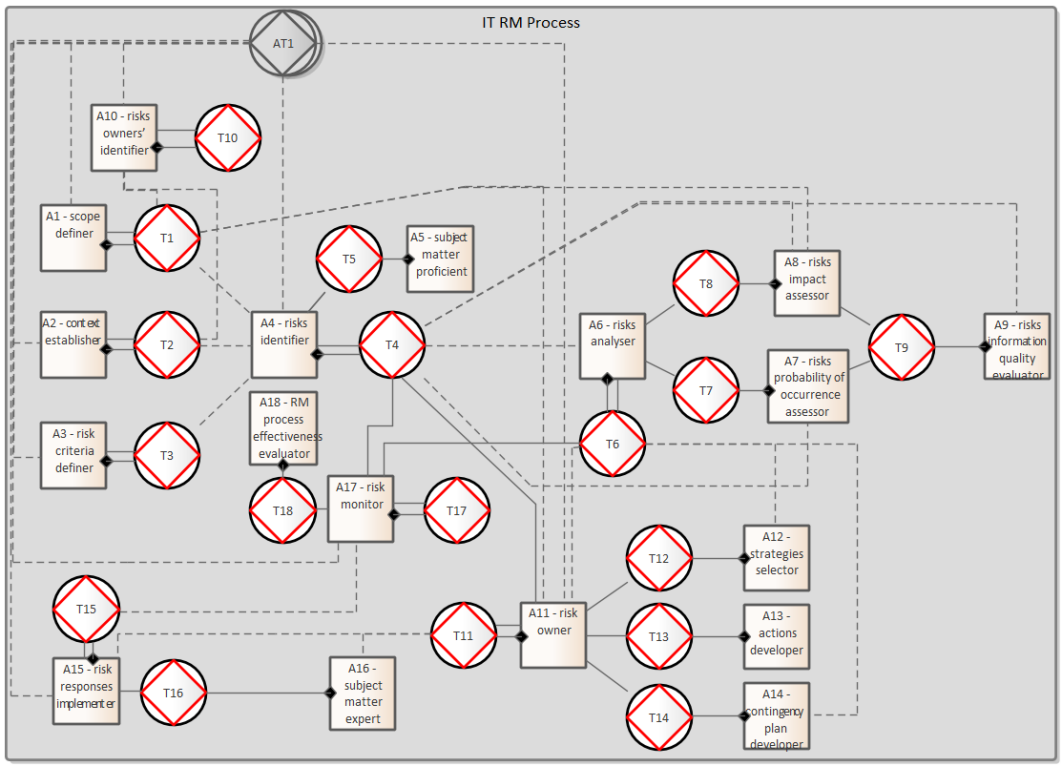

Figure 3. IT RM's Organization Construction Diagram.

model of an organization's state space and the transition space of its Production World (P-world). Regarding the *state space*, it contains all identified P-fact types (i.e. entity types, value types, among others) and existence laws. Concerning the *transition space*, the FM contains the production event types and occurrence laws. It is represented in an *Object Fact Diagram* (OFD) [5, 2].

The OFD, as shown in Figure 4, stipulates which facts are important in the P-world. The roundangles are classes (e.g. RISK). The red diamonds represent production event types. These are represented as unary predicates concerning an entity type or class. For instance, the event type "the impact of Risk is assessed" concerns the entity class RISK (or the entity type Risk). Property types are represented by lines between classes, for instance the property type "the risk owner of Risk is Risk Owner" is a function that maps RISK to RISK OWNER. The ">" specifies that RISK is the domain of the function and that RISK OWNER is the range. The class RISK is the main concept of IT RM, and the domain of five product kinds, P4, P6, P7, P8 and P9.

The Action Model (AM) was the last model to be produced. It is the ontological model of an organization's operation, and contains *action rules* that specify how C-facts must be responded [5, 2].

4. Conclusion

The advances of IT are allowing organizations to use new digital business models and to create new ways to leverage data for growth. These advances bring many opportunities to the organizations, but also bring challenges. Digitalization raises relevant policy challenges: privacy, security, jobs, skills, among others. So, an evolution in the organization's policies and practices is necessary to build and maintain trust [8].

One of the biggest challenges that come with expanding one's digital presence is addressing the security needs. Security needs are going through deep changes due to digital transformation since new security vulnerabilities appear frequently. In this context, organizations need a more proactive, continuously integrated and automated approach to security [8].

Due to the risks created by IT, IT RM became a must-to-do process. However, many organizations are not capable of implementing IT RM successfully. When we started studying IT RM we found out that IT RM is complex, since it encompasses many concepts/relationships, and the conceptual intersection between them is poor. Therefore, to simplify/clarify IT RM, we decided to produce an IT RM ontology.

Before producing an ontology we had to identify the

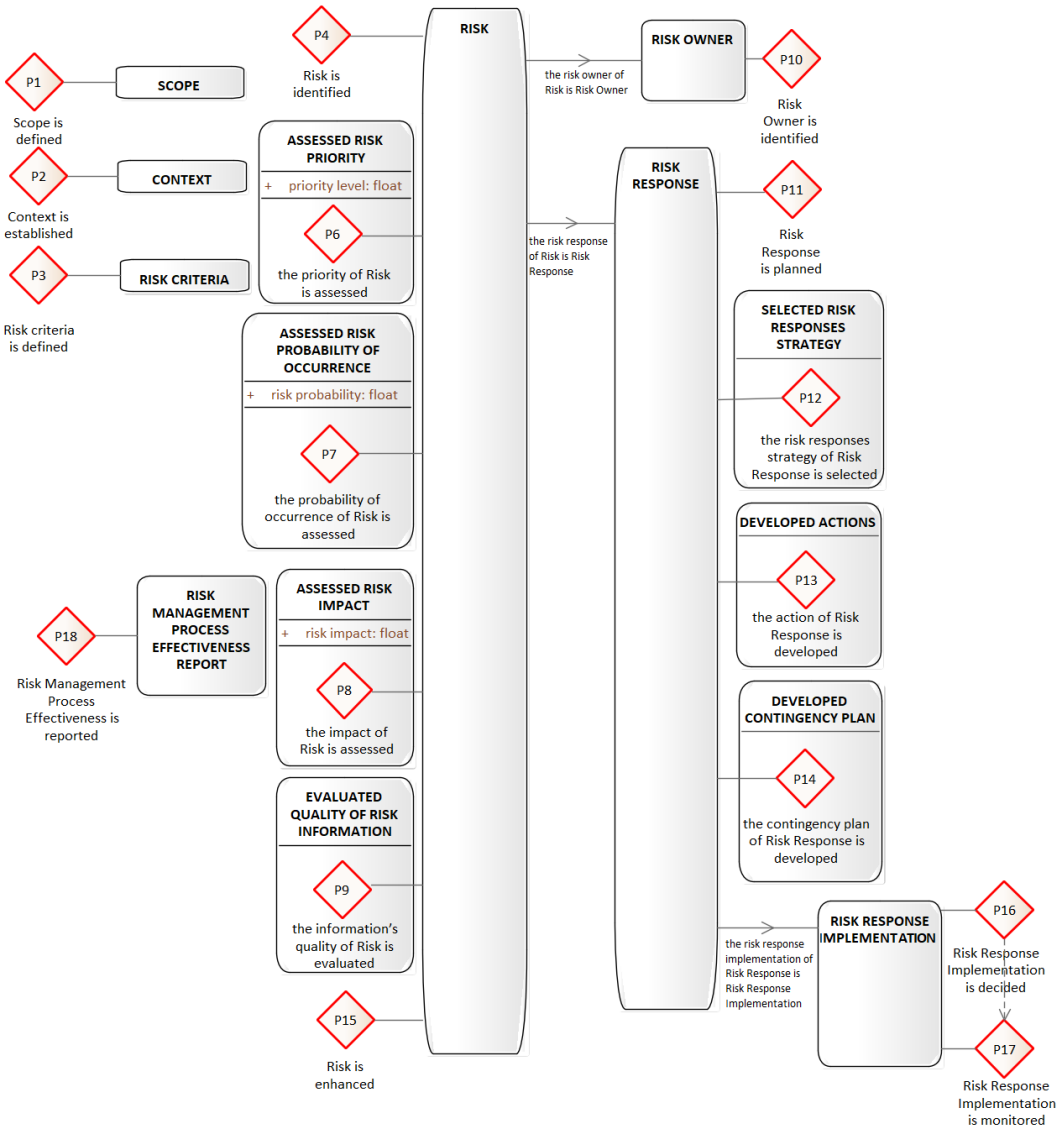

Figure 4. IT RM's Object Fact Diagram.

key concepts/relationships of IT RM. But, well-known standards are not consensual regarding the activities of IT RM. Moreover, many authors are continuously proposing new frameworks due to the limitations of these standards. Thus, an SLR was conducted in order to find out the key concepts/relationships of IT RM.

The SLR resulted on an IT RM process 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.

Then, an ontology of IT RM using DEMO was produced, through the analysis of the IT RM activities' definition resulting from the SLR.

DEMO has many benefits: provides clear guidelines; has a solid theoretical foundation, hence limiting the subjectivity in the modeling process; the models are simple since they use a restricted number of constructs and follow the transaction pattern, ensuring their completeness and integrity [9].

However, it has a number of potential disadvantages. One of the disadvantages concerns the understanding and implementation of DEMO models, because of its specific notation. So, these models may be difficult to understand at first for those unfamiliar with the notation. Additionally, since DEMO models do not contain any implementation-related details, using DEMO as a standalone for communicating and re-enacting IT RM process models to other parties is not advised [9].

This research contributes to the identification of the key concepts/relations of IT RM, and by simplifying/clarifying this process we increase the chances of a successful implementation of IT RM. The main goal of this paper is to show how it is possible to produce an ontology from the results of an SLR.

For future work, we will evaluate the completeness and validity of the IT RM ontology by deploying it to manage IT risks for a real case study. We will discuss if the ontology produced meets or does not meet the desired goals, by comparing its goals with the actual results from applying the ontology. Furthermore, key performance indicators will be defined and assessed to measure the success of applying the ontology.

Acknowledgements

The first and second author state that 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 (FCT) with reference UIDB/50021/2020 (INESC-ID). The third author state that this work is partially funded by national funds through FCT - Fundação para a Ciência e Tecnologia, I.P., under the project FCT UIDB/04466/2020.

References

[1] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele University*, vol. 33, no. 2004, pp. 1–26, 2004.

[2] J. L. Dietz and H. B. Mulder, *Enterprise Ontology: A Human-Centric Approach to Understanding the Essence of Organisation*. Springer Nature, 2020.

[3] I. ISO, "31000: 2018—risk management—guidelines," *ISO/TC*, vol. 262, 2018.

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

[5] A. Perinforma, "The essence of organisation. sapio," 2015.

[6] J. A. Hoogervorst, *Enterprise governance and enterprise engineering*. Springer Science & Business Media, 2009.

[7] J. Dietz and J. Hoogervorst, "Foundations of enterprise engineering," 2017.

[8] K. Matthews, *How digital transformation changes security needs*, 2019. `https://bit.ly/3ipEyR5`.

[9] P. Huysmans, K. Ven, and J. Verelst, "Using the demo methodology for modeling open source software development processes," *Information and Software Technology*, vol. 52, no. 6, pp. 656–671, 2010.

SLR bibliographic references

References

[1] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Computers & security*, vol. 44, pp. 1–15, 2014.

[2] J. J. Waring, "Constructing and re-constructing narratives of patient safety," *Social science & medicine*, vol. 69, no. 12, pp. 1722–1731, 2009.

[3] A. Olechowski, J. Oehmen, W. Seering, and M. Ben-Daya, "The professionalization of risk management: What role can the iso 31000 risk management principles play?," *International Journal of Project Management*, vol. 34, no. 8, pp. 1568–1578, 2016.

[4] T. Aven and V. Kristensen, "How the distinction between general knowledge and specific knowledge can improve the foundation and practice of risk assessment and risk-informed decision-making," *Reliability Engineering & System Safety*, vol. 191, p. 106553, 2019.

[5] S. V. Shrivastava and U. Rathod, "A risk management framework for distributed agile projects," *Information and software technology*, vol. 85, pp. 1–15, 2017.

[6] K. De Bakker, A. Boonstra, and H. Wortmann, "Does risk management contribute to it project success? a meta-analysis of empirical evidence," *International Journal of Project Management*, vol. 28, no. 5, pp. 493–503, 2010.

[7] S. Alhawari, L. Karadsheh, A. N. Talet, and E. Mansour, "Knowledge-based risk management framework for information technology project," *International Journal of Information Management*, vol. 32, no. 1, pp. 50–65, 2012.

[8] J. Wang, W. Lin, and Y.-H. Huang, "A performance-oriented risk management framework for innovative r&d projects," *Technovation*, vol. 30, no. 11-12, pp. 601–611, 2010.

[9] J. M. Yusta, G. J. Correa, and R. Lacal-Arántegui, "Methodologies and applications for critical infrastructure protection: State-of-the-art," *Energy policy*, vol. 39, no. 10, pp. 6100–6119, 2011.

[10] E. Kutsch and M. Hall, "Deliberate ignorance in project risk management," *International journal of project management*, vol. 28, no. 3, pp. 245–255, 2010.

[11] J. Teller and A. Kock, "An empirical investigation on how portfolio risk management influences project portfolio success," *International Journal of Project Management*, vol. 31, no. 6, pp. 817–829, 2013.

[12] D. C. Chou and A. Y. Chou, "Information systems outsourcing life cycle and risks analysis," *Computer Standards & Interfaces*, vol. 31, no. 5, pp. 1036–1043, 2009.

[13] S. A. Torabi, R. Giahi, and N. Sahebjamnia, "An enhanced risk assessment framework for business continuity management systems," *Safety science*, vol. 89, pp. 201–218, 2016.

[14] S. Andersen and B. A. Mostue, "Risk analysis and risk management approaches applied to the petroleum industry and their applicability to io concepts," *Safety Science*, vol. 50, no. 10, pp. 2010–2019, 2012.

[15] J. Oehmen, A. Olechowski, C. R. Kenley, and M. Ben-Daya, "Analysis of the effect of risk management practices on the performance of new product development programs," *Technovation*, vol. 34, no. 8, pp. 441–453, 2014.

[16] K. de Bakker, A. Boonstra, and H. Wortmann, "Risk managements' communicative effects influencing it project success," *International Journal of Project Management*, vol. 30, no. 4, pp. 444–457, 2012.

[17] Y. Kim and N. S. Vonortas, "Managing risk in the formative years: Evidence from young enterprises in europe," *Technovation*, vol. 34, no. 8, pp. 454–465, 2014.

[18] S. L. Vrhovec, T. Hovelja, D. Vavpotič, and M. Krisper, "Diagnosing organizational risks in software projects: Stakeholder resistance," *International journal of project management*, vol. 33, no. 6, pp. 1262–1273, 2015.

[19] J. Varajão, R. Colomo-Palacios, and H. Silva, "Iso 21500: 2012 and pmbok 5 processes in information systems project management," *Computer Standards & Interfaces*, vol. 50, pp. 216–222, 2017.

[20] M. Ghaffari, F. Sheikhahmadi, and G. Safakish, "Modeling and risk analysis of virtual project team through project life cycle with fuzzy approach," *Computers & Industrial Engineering*, vol. 72, pp. 98–105, 2014.

[21] B. Guertler and S. Spinler, "When does operational risk cause supply chain enterprises to tip? a simulation of intra-organizational dynamics," *Omega*, vol. 57, pp. 54–69, 2015.

[22] B. Kamsu-Foguem and P. Tiako, "Risk information formalisation with graphs," *Computers in Industry*, vol. 85, pp. 58–69, 2017.

[23] M. E. Kara, S. Ü. O. Fırat, and A. Ghadge, "A data mining-based framework for supply chain risk management," *Computers & Industrial Engineering*, p. 105570, 2018.

[24] L. Sundberg, "Electronic government: Towards e-democracy or democracy at risk?," *Safety science*, vol. 118, pp. 22–32, 2019.

[25] R. Slagmulder and B. Devoldere, "Transforming under deep uncertainty: A strategic perspective on risk management," *Business Horizons*, vol. 61, no. 5, pp. 733–743, 2018.

[26] H. P. Tserng, S. Y. Yin, R.-J. Dzeng, B. Wou, M. Tsai, and W. Chen, "A study of ontology-based risk management framework of construction projects through project life cycle," *Automation in construction*, vol. 18, no. 7, pp. 994–1008, 2009.

[27] J. Mu, G. Peng, and D. L. MacLachlan, "Effect of risk management strategy on npd performance," *Technovation*, vol. 29, no. 3, pp. 170–180, 2009.

[28] D. Aloini, R. Dulmin, and V. Mininno, "Modelling and assessing erp project risks: A petri net approach," *European journal of operational research*, vol. 220, no. 2, pp. 484–495, 2012.

[29] P. K. Dey, "Managing project risk using combined analytic hierarchy process and risk map," *Applied Soft Computing*, vol. 10, no. 4, pp. 990–1000, 2010.

[30] S. Islam, H. Mouratidis, and E. R. Weippl, "An empirical study on the implementation and evaluation of a goal-driven software development risk management model," *Information and Software Technology*, vol. 56, no. 2, pp. 117–133, 2014.

[31] G. J. Correa-Henao, J. M. Yusta, and R. Lacal-Arántegui, "Using interconnected risk maps to assess the threats faced by electricity infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 3-4, pp. 197–216, 2013.

[32] B. Barafort, A.-L. Mesquida, and A. Mas, "Integrating risk management in it settings from iso standards and management systems perspectives," *Computer Standards & Interfaces*, vol. 54, pp. 176–185, 2017.

[33] J. Meszaros and A. Buchalcevova, "Introducing ossf: A framework for online service cybersecurity risk management," *computers & security*, vol. 65, pp. 300–313, 2017.

[34] H. Leith and J. W. Piper, "Identification and application of security measures for petrochemical industrial control systems," *Journal of Loss Prevention in the Process Industries*, vol. 26, no. 6, pp. 982–993, 2013.

[35] F. Caron, J. Vanthienen, and B. Baesens, "A comprehensive investigation of the applicability of process mining techniques for enterprise risk management," *Computers in Industry*, vol. 64, no. 4, pp. 464–475, 2013.

[36] S. Ni, Y. Zhuang, J. Gu, and Y. Huo, "A formal model and risk assessment method for security-critical real-time embedded systems," *Computers & Security*, vol. 58, pp. 199–215, 2016.

[37] K. C. Demek, R. L. Raschke, D. J. Janvrin, and W. N. Dilla, "Do organizations use a formalized risk management process to address social media risk?," *International Journal of Accounting Information Systems*, vol. 28, pp. 31–44, 2018.

[38] B. Barafort, A.-L. Mesquida, and A. Mas, "Integrated risk management process assessment model for it organizations based on iso 31000 in an iso multi-standards context," *Computer Standards & Interfaces*, vol. 60, pp. 57–66, 2018.

[39] T. Yaqoob, A. Arshad, H. Abbas, M. F. Amjad, and N. Shafqat, "Framework for calculating return on security investment (rosi) for security-oriented organizations," *Future Generation Computer Systems*, vol. 95, pp. 754–763, 2019.

[40] Z. Ahmad, M. J. Thaheem, and A. Maqsoom, "Building information modeling as a risk transformer: An evolutionary insight into the project uncertainty," *Automation in Construction*, vol. 92, pp. 103–119, 2018.

[41] I. Kardes, A. Ozturk, S. T. Cavusgil, and E. Cavusgil, "Managing global megaprojects: Complexity and risk management," *International Business Review*, vol. 22, no. 6, pp. 905–917, 2013.

[42] S. D. Nogoorani and R. Jalili, "Tiriac: A trust-driven risk-aware access control framework for grid environments," *Future Generation Computer Systems*, vol. 55, pp. 238–254, 2016.

[43] S. Schmidt and S. Albayrak, "A quantitative framework for dependency-aware organizational it risk management," in *2010 10th International Conference on Intelligent Systems Design and Applications*, pp. 1207–1212, IEEE, 2010.

[44] S. Schinagl, R. Paans, and K. Schoon, "The revival of ancient information security models, insight in risks and selection of measures," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 4041–4050, IEEE, 2016.