IT Risk Management Ontology from representation to optimization using Enterprise Ontology

Mariana Sofia de Mendonça Rosa

Thesis to obtain the Master of Science Degree in

Information Systems and Computer Engineering

Supervisors: Prof. Sérgio Luís Proença Duarte Guerreiro
Prof. Rúben Filipe de Sousa Pereira

Examination Committee

Chairperson: Prof. Francisco João Duarte Cordeiro Correia dos Santos
Supervisor: Prof. Sérgio Luís Proença Duarte Guerreiro
Member of the Committee: Prof. Miguel Leitão Bignolas Mira da Silva

January 2021

Acknowledgments

First, I want to express my gratitude to my supervisor, Prof. Sérgio Guerreiro, for all the guidance, support, availability, and whose knowledge made this work possible. I also want to thank my co-supervisor Prof. Rúben Pereira, for all the guidance and support, specially in the first stage of this work.

I also want to thank Ana Rosa and Henrique Nemésio, who proofread all documents related to this research work and encouraged me through this journey.

I want to thank my parents for all the encouragement and motivation they gave me during this journey.

Lastly, I want to thank my friends from college for cheering me up during this work.

Abstract

Nowadays, organisations use and rely heavily on Information Technology (IT). Despite its benefits, IT inducts risks that could impact the achievement of the organisations' goals and their survival. Therefore, organisations implement Information Technology Risk Management (IT RM) to maximize the effectiveness of IT usage and manage IT-related risks.

However, IT RM's implementation is not easy since numerous standards, frameworks, and related literature propose Risk Management (RM) processes to deal with IT risks, composed of different activities, causing confusion. Moreover, organisations are not capable of managing risks successfully due to IT RM's complexity.

To overcome IT RM's complexity, this work proposes the definition of an IT RM ontology using Design and Engineering Methodology Ontology (DEMO), capturing the essential concepts/relationships of IT RM, that constitutes a positive step towards the simplification and clarification of this process, facilitating IT RM's enforcement. To find out the essential concepts/relationships of IT RM and overcome its diversity, this work proposes the performance of a Systematic Literature Review (SLR) following Kitchenham [2004] guidelines. The SLR results served as a basis to define the essential model of IT RM.

The Design Science Research Methodology was applied to design, develop, demonstrate, and evaluate the proposal.

The contributions of this work are: the extensive analysis of IT RM's essential concepts/relationships through an SLR; the identification of the benefits of using DEMO; a description of IT RM's essential model designed as an ontology; and a critical view of the benefits of the ontology proposed.

Keywords

DEMO, Essential Model, IT RM, Ontology, SLR

Resumo

Atualmente, organizações usam e dependem muito de Tecnologias de Informação (TI). TI traz benefícios, mas também induz riscos que podem afetar o alcance dos objetivos da organização e a sua sobrevivência. Por isso, as organizações implementam gestão de riscos de TI, de modo a maximizar a eficácia da sua utilização e gerir riscos de TI.

Todavia, a implementação de gestão de riscos de TI é difícil, pois vários padrões, *frameworks*, e literatura relacionada propõem processos de gestão de riscos para lidar com riscos de TI compostos por diferentes atividades causando confusão. Além disso, as organizações não gerem riscos com sucesso devido à complexidade deste processo.

Para superar a complexidade de gestão de riscos de TI, propõe-se a definição de uma ontologia utilizando *Design and Engineering Methodology Ontology* (DEMO), que capture os conceitos/relações essenciais deste processo, de modo a simplificá-lo e clarificá-lo, facilitando assim a sua aplicação. Para descobrir os conceitos/relações essenciais deste processo e superar a sua diversidade, propõe-se fazer uma revisão de literatura sistemática seguindo as diretrizes de Kitchenham [2004]. Os resultados desta revisão serviram de base para a definição do modelo essencial de gestão de riscos de TI.

Design Science Research Methodology foi aplicada para projetar, desenvolver, demonstrar e avaliar a proposta.

As contribuições deste trabalho são: análise profunda dos conceitos/relações de gestão de riscos de TI através da revisão de literatura sistemática; identificação dos benefícios de DEMO; descrição do modelo essencial do processo; e discussão dos benefícios da ontologia proposta.

Palavras Chave

DEMO, Modelo Essencial, IT RM, Ontologia, SLR

Contents

List of Figures

List of Tables

Acronyms

ACM	Association for Computing Machinery
AIS	Association for Information Systems
AM	Action Model
ARS	Action Rule Specifications
AS/NZS	Australian Standard for Risk Management
BCT	Bank Contents Table
C-act	Coordination act
C-fact	Coordination fact
C-world	Coordination World
CM	Construction Model
CNCS	Centro Nacional de Cibersegurança
CNPD	Comissão Nacional de Proteção de Dados
COSO	Committee of Sponsoring Organizations of the Treadway Commission
D-transaction	D-organisation transaction kind
DEMO	Design and Engineering Methodology Ontology
DEMOSL	DEMO Specification Language
DS	Design science
DSRM	Design Science Research Methodology
EE	Enterprise Engineering
EO	Enterprise Ontology
ERM	Enterprise Risk Management
FM	Fact Model
GDPR	General Data Protection Regulation

GSRM	Goal-driven Software Development Risk Management Model
I-transaction	I-organisation transaction kind
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INESC TEC	Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência
IS	Information Systems
ISO	International Organization for Standardization
ISPUP	Instituto de Saúde Pública da Universidade do Porto
IT	Information Technology
IT RM	Information Technology Risk Management
O-transaction	O-organisation transaction kind
OCD	Organisation Construction Diagram
OER	Organisational Essence Revealing
OFD	Object Fact Diagram
OSSF	Online Services Security Framework
P-act	Production act
P-fact	Production fact
P-world	Production World
PM	Process Model
PMBOK	Project Management Body of Knowledge
PSD	Process Structure Diagram
PSI	Performance in Social Interaction
RM	Risk Management
SLR	Systematic Literature Review
TPT	Transaction Product Table
WoM	Way of Modelling
WoO	Way of Organising
WoS	Way of Supporting
WoT	Way of Thinking
WoW	Way of Working

1

Introduction

Contents

Information Technology (IT) is considered an essential tool that can considerably affect the productivity of an organisation [3], and support its sustainability and growth [4]. IT is defined as “the application of technology to solve business or organisational problems on a broad scale” [5].

Nowadays, organisations are depending more than ever on IT to survive and grow. Organisations depend on IT since they have recognised its benefits to increase the quality, reliability, and speed of affairs and the importance of its employment in increasing the efficiency and effectiveness of the organisation. IT supports the existing business strategies of the organisation but also helps to form new strategies. IT is crucial for the success of daily operations and for gaining competitive advantage [4].

Besides the benefits that IT brings, IT also inducts risks. These risks can occur as a result of the deficiency or failure of internal proceedings, human resources, systems, or external events [6]. With the rising importance of IT, the weight of risks induced by IT rises [6].

The environment of organisations that rely on IT is complex and constantly changing due to the rapid pace of technological evolution. Therefore, organisations must manage IT risks effectively [7].

To manage the risks resulting from the dependency on IT, organisations have to implement Information Technology Risk Management (IT RM).

IT RM does not relate solely to the identification of risks, it is also concerned with the ability to anticipate, avoid, and mitigate issues emerging during the management of organisational tasks, for instance, decision-making regarding the application of IT. This has led to the creation of solutions centred around technology, people, and processes, aiming at reducing IT risks, thus ensuring that the organisation is compliant with current regulations and enabling the infrastructure to perform at a sustainable level [8].

Some organisations consider that IT RM is not a relevant process because not enough empirical evidence exists to prove the connection and causation between IT RM and success [9].

Additionally, some organisations opt to not implement IT RM due to factors such as difficulties in justifying the costs associated with the implementation of IT RM since the benefits of this process are not definite (e.g. money, time, manpower), lack of skills and familiarity of the managers in implementing IT RM, among others [10].

1.1 Problem definition

IT RM is a critical problem since it allows an organisation to manage risks that can deviate the organisation from its goals. However, organisations face difficulties in implementing this process.

In the last few years, IT RM has been a hot topic, which led to the creation of numerous standards and frameworks to assist organisations with its implementation. The problem is that these standards and frameworks propose Risk Management (RM) processes to deal with IT risks comprising different activities, resulting in some confusion regarding the concepts and relationships of IT RM. Moreover, these standards and frameworks have their own limitations, so the research community is continuously creating new frameworks [11].

Managers must understand the different concepts, relationships and practices involved in IT RM. The main obstacle for understanding it is that this process domain is complex since it encompasses many concepts and relationships, and the conceptual intersection between them is poor.

This research work aims at finding out the key concepts and relationships of IT RM, trying to reach consensus regarding this process, and at reducing the perceived complexity of IT RM.

1.2 Solution objectives

The main objective of this research work is to simplify and clarify IT RM and optimize its implementation through Enterprise Ontology (EO), which uses Design and Engineering Methodology Ontology (DEMO). DEMO is rooted in Enterprise Engineering (EE) theories that aim at reducing the complexity of any process or system [2].

However, it is not certain what should be modelled since there is a lack of consensus regarding IT RM's concepts and relationships, more particularly the activities that should be part of the process. Therefore, this research used the Systematic Literature Review (SLR) methodology, based on the guidelines of Kitchenham [2004], to review the essential and most popular RM activities implemented and proposed in the literature to deal with IT risks.

In summary, the objectives of this work are:

- To study, analyse, and compare the different IT RM activities through an SLR to determine which are the most popular and essential activities.
- To define an ontology of IT RM using DEMO in order to simplify and clarify this process by facilitating its design, implementation, and assessment. This will consequently increase the chances of a successful implementation of IT RM.

1.3 Research Methodology

Design science (DS) is a problem-solving paradigm with the purpose of designing, developing, demonstrating, and evaluating innovative and new IT artifacts that must solve identified organisational problems [1].

The Design Science Research Methodology (DSRM) integrates principles, practices, and procedures needed to perform the DS research, aiming at enhancing the production, presentation, and evaluation of this research [1]. DSRM was the approach chosen in this research work.

DSRM consists of six steps, namely [1]:

1. *Problem identification and motivation* - Specify the research problem and justify the solution's value;

2. *Define the objectives for a solution* - Deduce the objectives of a solution from the problem specification and knowledge of what is possible and achievable;

3. *Design and development* - Create artifact(s). These can either be constructs, models, methods, or instantiations;

4. *Demonstration* - Demonstrate the application of the artifact in solving one or more instances of the problem;

5. *Evaluation* - Observe and determine to what extent the artifact supports a solution to the problem;

6. *Communication* - Communicate the problem and its significance, the utility and novelty, design rigor and effectiveness of the artifact.

Figure 1.1 describes each DSRM step in the context of this work.

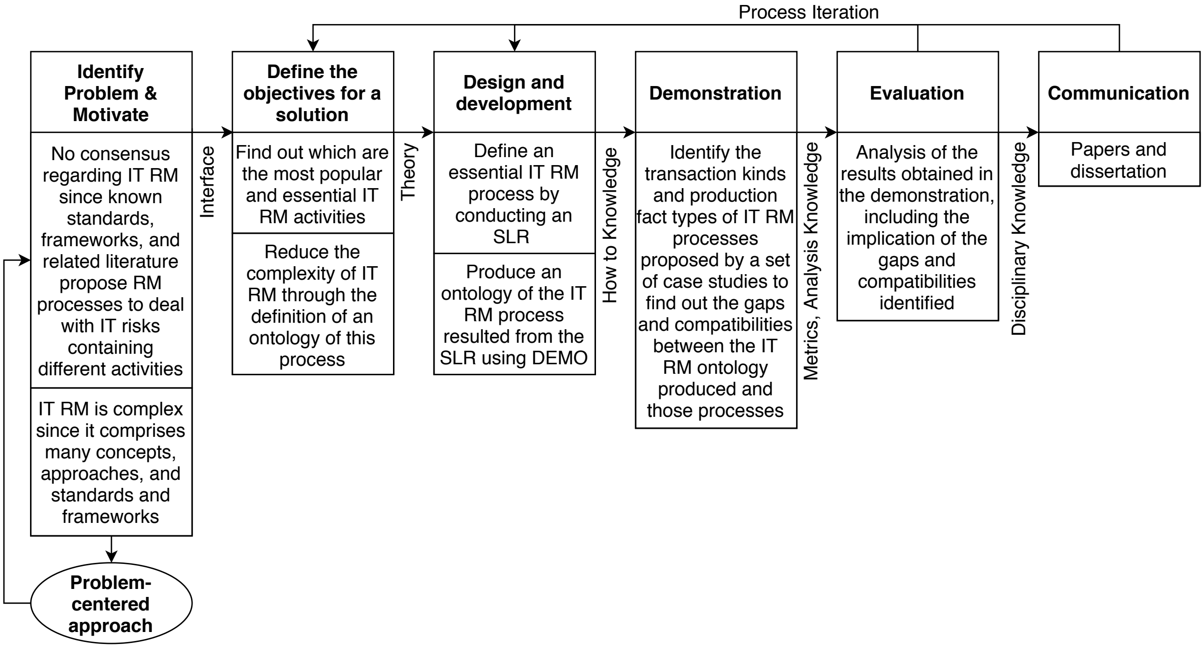
Process Iteration
Identify Problem & Motivate
No consensus regarding IT RM since known standards, frameworks, and related literature propose RM processes to deal with IT risks containing different activities
IT RM is complex since it comprises many concepts, approaches, and standards and frameworks
Problem-centered approach
Interface
Define the objectives for a solution
Find out which are the most popular and essential IT RM activities
Reduce the complexity of IT RM through the definition of an ontology of this process
Theory
Design and development
Define an essential IT RM process by conducting an SLR
Produce an ontology of the IT RM process resulted from the SLR using DEMO
How to Knowledge
Demonstration
Identify the transaction kinds and production fact types of IT RM processes proposed by a set of case studies to find out the gaps and compatibilities between the IT RM ontology produced and those processes
Metrics, Analysis Knowledge
Evaluation
Analysis of the results obtained in the demonstration, including the implication of the gaps and compatibilities identified
Disciplinary Knowledge
Communication
Papers and dissertation

Figure 1.1: DSRM cycle mapped to this research work adapted from [1]

1.4 Thesis Structure

The structure of this work is aligned with the six steps of the DSRM. This document is divided in seven chapters, described as follows.

- Chapter 1, Introduction - provides a contextualization regarding the subject of this research work, identifies and describes the problems and the solutions proposed to solve these problems concerning IT RM, and provides a brief description of the approach adopted to develop this work that is DSRM;
- Chapter 2, State of the Art - identifies and discusses concepts that are important to support the problems identified and the development of artifact(s). This chapter is split by concepts, namely IT RM and DEMO;
- Chapter 3, Systematic Literature Review - explains the planning and execution of the SLR conducted to overcome IT RM's diversity and the analysis and conclusions of the results obtained;
- Chapter 4, Design and Development - presents and describes the ontology of IT RM produced to overcome this process's complexity;
- Chapter 5, Demonstration - presents the results of identifying gaps between the transaction kinds and production fact types of the IT RM ontology and the IT RM processes of three case studies;
- Chapter 6, Evaluation - analysis of the implications of the gaps, namely lack and excess of elements, identified in the previous chapter and explanation of what was learned based on the results obtained;
- Chapter 7, Conclusion - presents the main scientific contributions of this research work, the papers that were submitted to the scientific community, the limitations established, and some proposals for future work.

2

State of the Art

Contents

This chapter describes IT RM and its importance (Section 2.1). Additionally, it explains the principal theoretical notions and definitions regarding this research work so the reader can have a better understanding of the concepts that are the basis of this work. It also describes DEMO, including an overview of its theory and how it works (Section 2.2).

2.1 Information Technology Risk Management

With the creation of IT, the principal activity of an organisation is currently focusing on the ability to maintain and manage knowledge and information [12]. The maintenance and management of information is done by Information Systems (IS), which is a vital component in modern organisations since it is present in almost every business aspect. IS can improve productivity and the decision-making process, reduce operational costs, gain competitive advantage, among other benefits [9].

IS and IT are directly connected, given that IS decides the IT requirements for its operation, while IT influences a change in the IS when a new technology emerges, so it is vital for organisations to implement an efficient IT management if the organisation desires to deliver IS without disturbances [12].

Nowadays, organisations depend on IT to survive in the current economy. Despite the benefits of this dependency, it also causes risks that can affect the achievement of the organisation's goals. Risk is usually defined as the "effect of uncertainty on objectives", either negative or positive [13]. Therefore, to boost the effectiveness of IT usage and to manage the risks associated with it, organisations implement IT RM, a specialisation of RM. RM is defined as "coordinated activities to direct and control an organisation with regard to risk" [13].

In IT RM, RM activities are implemented to recognise, identify and control events that can affect the achievement of the organisation's goals by dealing with IT risks, such as leakage and modification of information, disruption or annihilation of critical IT services, loss of computer system data, wrong software load, among others [14, 15].

If an organisation can successfully manage risks, it can change them so that the organisation is more likely to meet its goals. Hence the need for organisations to implement IT RM [16].

However, organisations face difficulties in implementing IT RM. First, standards, frameworks, and related literature propose different and general RM processes to deal with IT risks, causing confusion regarding the concepts (more specifically the activities) and relationships of IT RM. Additionally, these standards and frameworks have limitations, therefore the research community is constantly proposing new frameworks [11]. Second, IT RM is complex since it comprises numerous activities and concepts.

2.2 Design and Engineering Methodology Ontology

DEMO is the principal theory in the discipline of EE and it is widely accepted in both scientific research and practical appliance. It allows the definition of an ontology systematically, and it offers a significant reduction of the process complexity. An ontology aims at providing a basis for the overall understanding of some area of concern within a group of people who may not know each other and who may have completely different cultural backgrounds [2].

DEMO has many benefits: (a) offers clear guidelines; (b) has a strong theoretical foundation, thus restricting the subjectivity in the modelling process; (c) the models are simple since they use a limited number of constructs, and follow the transaction pattern ensuring completeness and integrity [17].

As presented in Figure 2.1, the core of DEMO includes a Way of Modelling (WoM) composed of four *aspect models* and a Way of Working (WoW) that offers the Organisational Essence Revealing (OER) method. The WoM and the WoW are rooted in a common Way of Thinking (WoT) that consists of some EE theories. It can be complemented with a Way of Organising (WoO) that relates to the manner in which this theory's application is organised and managed, and a Way of Supporting (WoS) that contains software tools that support the WoM and WoW. The WoW supports the making of *essential models*. This implies that DEMO is mainly about EO [2].

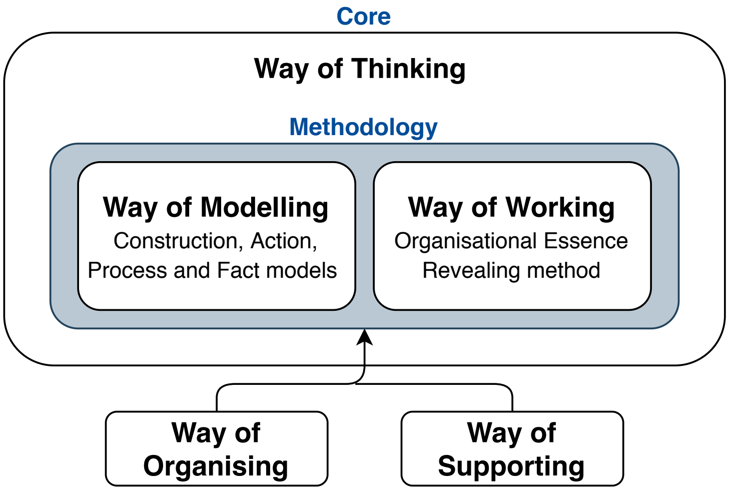

Figure 2.1: DEMO specified in the Five Ways Framework adapted from [2]

2.2.1 Theory

According to "Enterprise Ontology: A Human-Centric Approach to Understanding the Essence of Organisation" [2], nowadays, it is challenging for businesspersons to succeed without a fundamental, systematic, and integral comprehension of how organisations operate. An organisation's conceptual model is required to deal with current and future challenges. This conceptual model must be coherent, comprehensive, consistent, and concise, and only displaying the organisation's essence.

By exerting the notion of EO, one acquires an understanding of the organisation's essence that is *coherent* (the four aspect models form a rational and truly integral whole), *comprehensive* (all significant matters are covered), *consistent* (the four aspect models are clear from discrepancies and inconsistencies) and *concise* (no superfluous matters are included in the conceptual model). The main feature, though, is that this conceptual model is called an *ontological model* and it is *essential*, displaying only the organisation's essence, regardless of all implementation and realisation aspects.

EO has a strong scientific foundation and offers a significant reduction of complexity, which results in a comprehensive overview and deep understanding of organisations, and their constructions and operations. Thus enabling one to achieve *intellectual manageability*, which is one of the general goals of EE. EO is one of the conceptual pillars of the discipline of EE. EO focuses on essence and simplicity, and it uses DEMO. The concept of essence is addressed by some EE theories, being one of them the Performance in Social Interaction (PSI) theory that focus on the essence of organisations.

According to PSI theory, every organisation is a social system, meaning that the elements of the system are social individuals (actors). The social system's operating principle consists of the ability of actors to enter into and comply with commitments towards each other.

An *actor* is a subject (human being) in an actor role. The *actor role* specifies the authority that the actor may exercise and the responsibility to do so. Commitments are raised in Coordination act (C-act)s, and these consist of a performer, an intention, an addressee, and a product. Both *performer* and *addressee* are human beings with the ability to participate in and comply with commitments. The *proposition* “is a state of affairs that is or that can be the case”. For example, in the context of a pastry shop, the proposition can be "client has got a croissant". The *intention* is the performer's intent (a client in Figure 2.2) regarding the addressee (a waiter) concerning the proposition. If the intention is 'request', the performer wants the addressee to turn the proposition true. In the pastry shop example, the client wants the waiter to bring a croissant to the client [18].

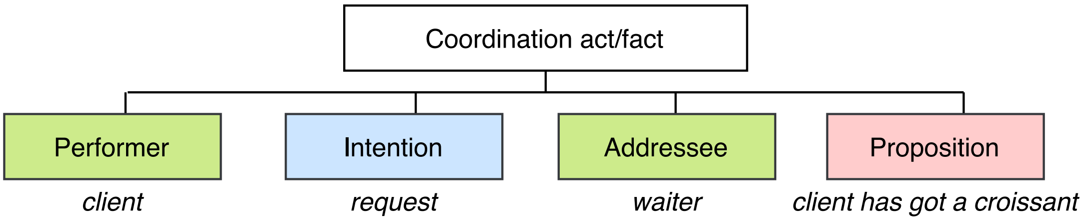

Figure 2.2: The structure of a Coordination act/fact adapted from [2]

When carrying out a C-act, the performer raises three validity claims towards the addressee: the claim to justice, the claim to sincerity, and the claim to truth. These claims must be evaluated by the addressee, and the outcome of this evaluation will guide the addressee in their response. By accepting the *claim to justice* in Figure 2.2, the waiter acknowledges the client's authority to make the request. By accepting the *claim to sincerity*, the waiter believes that the client is being sincere and trustworthy in making the request. By accepting the *claim to truth*, the waiter expresses their capability in making the proposition true. If all three claims are accepted, the waiter responds with a promise. Otherwise, the waiter will decline the client's request [18].

The outcome of performing a C-act is the creation of the corresponding Coordination fact (C-fact). In Figure 2.2, the C-fact is having requested a croissant. C-acts and C-facts always take place in specific patterns of interaction between actors in two roles (initiator and executor), called transactions. A *transaction* involves three phases: in the *order phase*, both actors will reach to an agreement regarding the product that the executor can promise to bring about in response to the initiator's request; in the *execution phase*, the executor will produce the product; and in the *result phase*, both actors will negotiate and settle with each other on the delivered product, this is performed by the following C-acts: state (executor) and accept (initiator).

Every transaction is of a particular transaction kind. A *transaction kind* relates to one particular *product kind* and has one particular actor role as its executor role [18]. The combination of a transaction kind and its executor role is called a *transactor role*.

C-acts are always about Production fact (P-fact)s, for example, one may request, promise, state, and accept the P-fact *Marta has got the best paper award of the Conference*. When the subjects of an organisation perform Production act (P-act)s, they create products (P-facts), for example, a P-act can be the preparation of a cup of tea and the corresponding P-fact is the cup of tea. Every P-fact is the outcome of a successfully completed transaction. A P-fact is an instance of a P-fact type (or product kind), for example the P-fact 'membership 23 is started' is an instance of the P-fact type 'Membership is started'. The becoming existent of a fact is called an *event* (change of state).

P-acts can be original, informational, and documental. *Original P-acts* bring about original, new P-facts. These acts include manufacturing things, transporting, observing, devising, deciding, and judging. *Informational P-acts* comprehend remembering facts and computing or deriving facts. *Documental P-acts* involve the data that hold facts and the files that carry the data. These acts include saving, supplying, and converting (documents or data) and storing, recovering, copying, transmitting, and destroying (files). Since original acts are the only ones that modify the Production World (P-world)'s state of an organisation, these must be carried out by authorised and responsible actors, hence subjects in actor roles.

The actors of an organisation can be split up into three layers, based on the distinction of the three sorts of P-acts: 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.

The realisation aspect of an organisation is understood as the devising of the I-organisation and the D-organisation, given its O-organisation. Contrary, abstracting from realisation yields the organisation's O-organisation. Moreover, abstracting from implementation yields the ontological model of the organisation's O-organisation that is its *essential model*. The essence of the organisation is captured in its O-organisation.

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

2.2.2 Methodology

As previously mentioned in Section 2.2, the core of DEMO is composed of a WoM (aspect models in which the ontological knowledge of the organisation is demonstrated) and a WoW (method for the development of the ontological aspect models).

2.2.2.A Aspect Models

According to "Foundations of enterprise engineering" [18] and "Enterprise Ontology: A Human-Centric Approach to Understanding the Essence of Organisation" [2], the ontological model of an organisation in DEMO Specification Language (DEMOSL)-3 consists of four integrated aspect models: Construction Model (CM), Process Model (PM), Fact Model (FM) and Action Model (AM).

The CM is the ontological model of an organisation's construction: the *interaction structure* (i.e. the transaction kinds between internal actor roles, and between these and external actor roles), the associated actor roles, and the *interstriction structure* (i.e. the information links from internal actor roles to the transaction kinds).

The PM is the ontological model of an organisation's state and transition spaces of the Coordination World (C-world). Concerning the state space, this model comprises existence laws and process step kinds that the organisation applies to the transaction kinds, according to the complete transaction pattern, while regarding the transition space, the PM consists of the coordination event kinds and applicable occurrence laws.

The FM is the ontological model of an organisation's state and transition spaces of the P-world. Regarding the state space, this model comprises all identified P-fact types and existence laws, while concerning the transition space, the FM consists of the production event types, as well as the applicable occurrence laws.

The AM is the ontological model of an organisation's operation, it comprises *action rules*. Action rules describe the C-acts/P-acts that must be executed and the C-facts/P-facts that must be assessed.

2.2.2.B Organisational Essence Revealing method

The method that supports the creation of essential models in DEMO is called the OER method.

According to “Enterprise Ontology: A Human-Centric Approach to Understanding the Essence of Organisation” [2], the first step of this method is to distinguish between the three human abilities that actors exert when carrying out C-acts: performa, informa, and forma. The distinction of these abilities corresponds to the three distinct sorts of P-acts: original, informational, and documental. The main objective of this step is to determine the transaction kinds and the actor roles in the O-organisation. This step consists of crossing the available documentation and highlighting parts of the text that expresses performa or informa or forma matters.

The next step involves identifying the relevant transaction kinds, and corresponding product kinds, and executing actor roles, based on the highlights done in the previous step.

After completing the second step, it is possible to build the essential model since one has all transaction kinds and their executing actor roles in the O-organisation.

The last step is the essential model’s validation, where one verifies if the model is correct according to the applied theory and ensures that the model offers an honest understanding of the modelled piece of reality.

2.3 Summary

The advances of IT bring many advantages to the organisations, but also bring risks. Due to the risks created by IT, IT RM became a must-to-do process. However, many organisations are not capable of implementing IT RM successfully, due to this process’s diversity and complexity.

DEMO, has one WoT comprising EE theories, a WoM consisting of four aspect models, and a WoW consisting of a method. Together they offer the support that is required to develop essential models of organisations [2].

EO provides conceptual and high-quality models since it focuses only on the organisation’s essence, abstracting from all implementation and realisation aspects [19].

So, by having its roots on EO, one of the conceptual pillars of EE, when developing an essential model using DEMO one acquires an understanding of the organisation’s essence that is comprehensive, coherent, consistent, and concise [2].

3

Systematic Literature Review

Contents

3.1 Introduction

To overcome IT RM's diversity, an SLR was conducted. The main goal of this SLR is to answer the following question: Which are the most proposed and essential IT RM activities and their relationships?

The purpose of an SLR is to identify, evaluate, and interpret all available research relevant to a research question [20], in this case, the activities involved in the implementation of IT RM. This type of review is considered superior to traditional reviews since it brings more transparency and rigor [21]. The SLR allows reducing selection bias when choosing publications, which in turn improves the legitimately and validity of the findings. Therefore, another reason for conducting the SLR is to synthesize existing literature regarding IT RM "a manner that is fair and seen to be fair" [22].

With the purpose of addressing this research goal, an SLR, following Kitchenham guidelines [2004] [20], was conducted. Tasks taken to conduct this review are shown in Table 3.1.

Table 3.1: 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 varied, with no consensus regarding the activities that can compose this process	Filters' application and final articles: 50 articles	Findings report: Discussion about the gathered data and draw conclusions
Research question: Which are the most proposed and essential IT RM activities and their relationships?	Data extraction and analysis: Reading and further analysis of the articles resulted in the final set of 44 articles Sample characteristics Extraction of information regarding IT RM concepts/relationships	
Review protocol: Search string; Filters; Repositories; Inclusion criterion		

This chapter outlines the SLR used to gather information, including the planning (Section 3.2) and how the review was conducted (Section 3.3), the set of final articles obtained and these articles' analysis, and consequent results (Section 3.4).

3.2 Planning Systematic Literature Review

In the planning phase, the goals of the SLR were established and the way in which the SLR will be performed was decided. Before searching for literature associated with the research question, the search terms were defined.

The keywords defined were: *"IT Risk Management" AND ("activities" OR "process" OR "stages" OR "frameworks" OR "standards")*. These were used as strings and the main keyword for all the strings was *"IT Risk Management"*.

Before performing this review, when first studying IT RM, it was noticed that many of the IT RM activities proposed are based on frameworks and standards, such as International Organization for Standardization (ISO) 31000, Project Management Body of Knowledge (PMBOK), Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM), among others. Therefore, it was added the “frameworks” and “standards” keywords to the set of search terms, to obtain the activities of IT RM that had a greater “impact” in the research community by following known frameworks and standards.

Four electronic repositories were selected, to obtain information regarding the essential activities of IT RM and their relationships:

- Association for Computing Machinery (ACM) (https://dl.acm.org);
- Association for Information Systems (AIS) (https://aisel.aisnet.org/jais/);
- Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library (https://ieeexplore.ieee.org);
- ScienceDirect (https://www.sciencedirect.com).

After defining the keywords and choosing the repositories, the searching process began. First, a search with the chosen keywords in each repository was performed without any filter. Then, five filters were created and applied following this order:

1. Search for the keywords in the article’s title, or abstract, or article’s author keywords;
2. Remove duplicate articles in the same repository and between repositories;
3. Eliminate articles that were not in English, that were not from Journals or Scientific Magazines and Conferences, and articles published before 2009;
4. Remove articles published in lower-ranked publications or journals, ensuring that the articles selected were high-quality peer-reviewed. Articles from publications/journals that are highly cited by the scientific community indicate a higher degree of confidence in the research work done and that it is peer-reviewed;
5. Manually assess articles’ abstract and introduction.

3.3 Conducting Systematic Literature Review

As mentioned in Section 3.2, the articles that resulted from the research made with the keywords needed to “proceed” through five filters in each repository. The flow of the filtering process, including the number of articles obtained in each repository and after applying each filter, is presented in Figure 3.1.

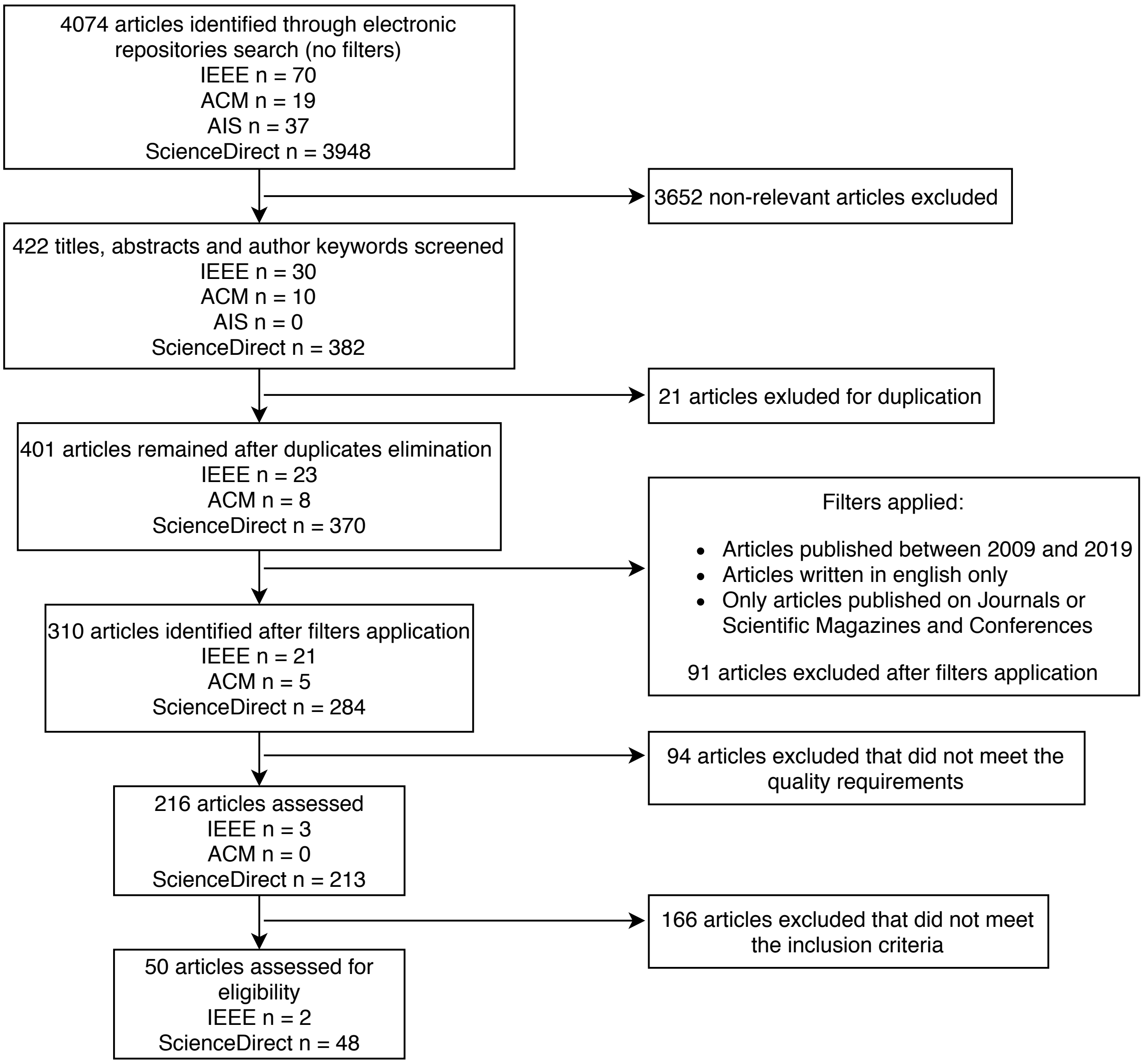
4074 articles identified through electronic repositories search (no filters)
IEEE n = 70
ACM n = 19
AIS n = 37
ScienceDirect n = 3948
3652 non-relevant articles excluded
422 titles, abstracts and author keywords screened
IEEE n = 30
ACM n = 10
AIS n = 0
ScienceDirect n = 382
21 articles exluded for duplication
401 articles remained after duplicates elimination
IEEE n = 23
ACM n = 8
ScienceDirect n = 370
Filters applied:
• Articles published between 2009 and 2019
• Articles written in english only
• Only articles published on Journals or Scientific Magazines and Conferences
91 articles excluded after filters application
310 articles identified after filters application
IEEE n = 21
ACM n = 5
ScienceDirect n = 284
94 articles excluded that did not meet the quality requirements
216 articles assessed
IEEE n = 3
ACM n = 0
ScienceDirect n = 213
166 articles excluded that did not meet the inclusion criteria
50 articles assessed for eligibility
IEEE n = 2
ScienceDirect n = 48

Figure 3.1: Flow of filtration process

The application of the first filter had the goal of obtaining all articles which have the defined keywords in their main topic, that is why only articles with these keywords in the title, or abstract or author keywords are selected since these three sectors summarize the article's topic. With the application of this filter, it was possible to discard a substantial number of articles, remaining only 422 articles from the 4074 articles initially obtained.

The second filter removed duplicate articles in the same repository and between repositories, resulting in a set of 401 articles.

The third filter eliminated articles that were not in English, since it is not feasible to translate publications issued in foreign languages, that were not published in Journals or Scientific Magazines and Conferences, and articles published before 2009 since IT RM is a subject that has been highly studied and developed in the past 10 years. This restricted period guarantees that the set analysed consists of recent publications. Consequently, 91 articles were excluded.

In the fourth filter, articles were ranked by their publication rank, which resulted in 216 articles. This filtering process made use of Scimago (https://www.scimagojr.com) and Conference Ranks (http://www.conferenceranks.com/#data), since these provide journals and conferences ranks, respectively. 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.

Finally, in the fifth filter, the abstract and introduction of the articles obtained with the previous filter were read and evaluated by a new inclusion criterion, which resulted in 50 articles. The inclusion criterion used was the selection of articles that covered the implementation of RM to IT risks. This included articles that, implicitly or explicitly, stated IT RM activities and articles that adopted an IT RM process proposed by known frameworks and standards. The articles that did not meet this condition, such as [23], were excluded.

After the filtering process, the 50 articles that resulted from the filtration were subject to further analysis. For each article, the following data was extracted: IT RM process activities and, if applicable, which framework or standard were those activities from; the article's author; and other components of IT RM. Six articles were then removed from the final set of articles since these: focused on IT problems after the IT risks occurred; described methods and strategies that in future search might integrate an IT RM process, not yet specifying the activities that compose the process; refer to IT risks and RM, but do not specify an IT RM process to be applied to.

The final set of articles is composed of 44 articles.

Although IT RM has been highly studied and developed in the last ten years, there is still not a lot of data about this process in popular electronic repositories that contain diverse IT data, such as ACM, AIS and IEEE Xplore Digital Library. Because of that, the set of articles resultant from the SLR was small.

3.3.1 Sample characteristics

The sample contains 44 articles published in journals and conference proceedings. The main contributors of this research, as it can be observed in Figure 3.2, are articles from journals since only 5% of the articles are from conference proceedings.

In Table 3.2, which represents the distribution of the final articles by their publication rank, it can be observed that articles from all publication ranks were considered for this research. As illustrated, 35 articles are from journals belonging to the Q1 rank, which is the main rank in the final articles.

As described in Section 3.3, if an article was assessed by both ERA and Qualis ranking, Qualis would prevail. So, Table 3.2 only shows Qualis ranking even if the articles were assessed by both rankings.

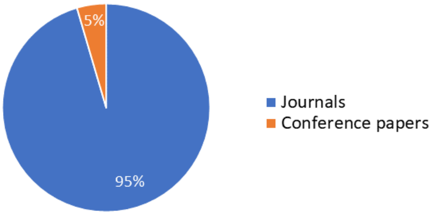

Figure 3.2: Distribution of publication type

Table 3.2: Final articles by publication rank

Journal rank	Total
Q1	35
Q2	7
	42

	Conference rank	Total
Qualis	A1	1
	B2	1
		2

A total of 113 different authors were identified from the final set of articles. Most authors published one article since only 12 authors participated in more than one article from the final set, which suggests that there is a great diversity of views and opinions regarding IT RM.

3.4 Reporting the Reviews

The goal of this discussion is to find which are the essential activities of IT RM and extract conclusions about those. First, the knowledge acquired during the analysis of the final set of articles is described. Then, it will be explored how the different IT RM activities proposed relate to each other.

3.4.1 Results

The results of the SLR include the definition of concepts and a detailed explanation of the carried-out research; a discussion regarding the IT RM activities; and a discussion about the frameworks and standards that propose those activities.

Several key concepts were extracted from the articles resulted from the SLR, namely the IT RM activities and the frameworks and standards that support these activities. However, in some articles there is a lack of clarification about the IT RM activities implemented or proposed.

3.4.1.A Activities

During the analysis of the final set of articles, it was evident that the activities that should be part of IT RM are still not well established. To further analyse the content of each article, Table 3.3 was designed with the IT RM process activities proposed by each article. Some articles were not considered in Table 3.3 since they did not state the activities involved in the IT RM process, they only stated that the process was based on frameworks, standards or practices. These articles are [24], [25], [26] and [27].

The information gathered during the articles' analysis, regarding the IT RM activities presented by those articles could not be extracted directly, since this information is occasionally not explicit in the text.

In Table 3.3, it can be verified that the number of activities, that are part of the processes proposed by the final set of articles, differs. This inconsistency shows the lack of consensus regarding IT RM. Additionally, there is a big diversity of activities that can compose IT RM since a total of 74 different activities was identified, not counting with the activities highlighted in bold that belong to other activities. Note that some articles proposed the same IT RM process, namely [37] and [7], and [54] and [56].

Despite the variety of activities that compose the IT RM process, the following ten activities were the most frequent: Risk Identification; Risk Assessment; Risk Analysis; Risk Treatment; Risk Responses Planning; Context Establishment; Risk Response; RM Planning; Risk Control; Monitor and Control Risk.

Risk Identification is the most present activity in the IT RM processes proposed by the articles. Risk Identification has the purpose of determining which possible risks might affect the project and of documenting their characteristics [29]. This activity usually depends on activities such as Establishing the Context (ISO 31000:2009), RM Planning (PMBOK 5) and Scope Establishment (proposed by [29]).

During the analysis of the IT RM activities, it was noticed that some articles propose activities with different names but with the same meaning or purpose and that there are dependencies between them.

Some articles give the same meaning to Risk Analysis and Risk Assessment and others state that Risk Analysis belongs to Risk Assessment. Risk Analysis is an activity that facilitates the conversion of risk data into decision making information. It analyses the risks identified in a previous activity, usually Risk Identification. The probability of occurrence and impact of each identified risk should be estimated, either quantitatively or qualitatively, so that these risks can be categorized [29]. It is an activity that sometimes is not considered useful, especially quantitative risk analysis, since many of the risks in IT projects are not based on probability, but are epistemic, which means that there is not enough information available to make a decision [28]. Risk Assessment measures the risk's likelihood of occurrence and severity of consequence [31]. This activity is proposed by ISO 31000:2009 and COSO ERM. According to ISO 31000:2009, Risk Assessment is the overall process of Risk Identification, Risk Analysis and Risk Evaluation, and depends on Establishing the Context, while COSO ERM states that Risk Assessment depends on Event Identification.

In some articles, the activities Risk Assessment and Risk Analysis could be composed of other activities (highlighted in bold in Table 3.3). Risk Assessment could comprehend: Risk Identification; Risk Analysis; Risk Quantification; Risk Evaluation; System characterization; Threat Identification; Vulnerability Identification; Control Analysis; Likelihood Determination; Impact Analysis; Risk Determination; Control Recommendations; Results Documentation. While Risk Analysis can be divided into Quantita-

[1] Only a subset of all the IT RM activities is presented in Table 3.3, a full list is available at: `https://bit.ly/32Cozdm` (see the correspondence between the articles' index and its reference in SLR article references).

Table 3.3: IT RM activities, that were mentioned more than once, presented by each article (the symbol ● means that the IT RM activity is referred in the article)[1]

Article Reference IT RM activity	[28]	[29]	[30]	[31]	[32]	[33]	[34]	[35]	[15]	[36]	[37]	[38]	[39]	[7]	[9]	[40]	[41]	[42]	[43]	[44]	[45]	[46]	[47]	[48]	[49]	[11]	[50]	[51]	[52]	[53]	[54]	[55]	[56]	[57]	[14]	[58]	[59]	[60]	[61]	[62]	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 Responses 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

tive Risk Analysis and Qualitative Risk Analysis [46].

Risk Treatment is where an effective strategy to manage risks is selected and implemented [48]. This activity is proposed by ISO 31000:2009 and, according to this standard, depends on Risk Assessment.

Risk Responses Planning assists in transforming risk information into actions and judgments. It aims to reduce the probability of risk occurrence, to reduce the loss degree, and to change the risk consequences [29]. Risk Responses Planning is proposed by PMBOK 5 and, according to this standard, it depends on Qualitative Risk Analysis and Quantitative Risk Analysis.

Risk Response helps the project manager on the development of actions and techniques to mitigate the identified risks, enables the project manager to keep track of those risks, to identify new risks throughout the project and to implement risk response plans [32]. This activity is proposed by COSO ERM and, according to the standard, it depends on Risk Assessment. Risk Treatment, Risk Responses Planning and Risk Response are very similar, with only small variations, and in Table 3.3 it can be observed that they are never put together in the same IT RM process.

Monitor and Control Risk is the activity where the effectiveness of responses is verified and where new risks are identified and evaluated [46].

Risk Control is about monitoring and revising project risks, communicating and consulting [48]. This activity is like Monitor and Control Risk, except in article [42] where Risk Control means the same as Risk Treatment [42]. Risk Control is proposed by PMBOK 5 and depends on Risk Responses Planning.

During Context Establishment, the organisation defines its objectives, determines external and internal factors to be considered when managing risk, and sets the scope and risk criteria for the remaining process [51]. This activity is proposed by ISO 31000:2009.

RM Planning is the activity where the organisation's environment is reviewed, together with the organisational process assets, and project goals and objectives [46]. This activity is proposed by PMBOK 5. Context Establishment and RM Planning are very similar and are never put together in the same IT RM process, as can be seen in Table 3.3.

3.4.1.B Standards and Frameworks

Some articles integrated activities into their IT RM based on known frameworks or standards, that are crucial tools which support organisations while they are implementing their IT RM process. However, these have their limitations, which leads to the constant creation of new ones. Some articles from the final set suggested new frameworks for IT RM.

As shown in Table 3.4, 23 different standards and frameworks were identified on the final set of articles. The frameworks in bold were created and proposed by the article's authors. The standards and frameworks more frequently adopted were: ISO 31000:2009, PMBOK 5 and COSO ERM.

Table 3.4: Standards and Frameworks that support the IT RM activities presented in the final set of articles (the symbol • represents that the standard or framework is referred in the article)

Article Reference Standards/Frameworks	[29]	[30]	[31]	[32]	[33]	[48]	[15]	[37]	[38]	[11]	[50]	[9]	[51]	[52]	[53]	[40]	[54]	[55]	[56]	[42]	[43]	[57]	[14]	[59]	[46]	[27]	[60]	[61]	Total
ISO/IEC 31000:2009			•					•					•							•		•							5
PMBOK 5				•					•			•				•													4
COSO ERM																	•		•					•					3
NIPP - United States National Infrastructure Protection Plan			•								•																		2
Knowledge-Based Risk Management Framework (RiskManIT)	•																												**1**
Performance-oriented risk management framework		•																											**1**
AS/NZS, 1999 – Australian Standard for Risk Management			•																										1
The Standard for Portfolio Management					•																								1
Project Management Association						•																							1
ISSO 31010, 2009							•																						1
Project Risk Analysis and Management Guide									•																				1
Goal-driven Software Development RM Model (GSRM)										•																			**1**
Directive 2008/114/EC											•																		1
ISO 21500:2012												•																	1
Online Services Security Framework (OSSF)														•															**1**
NIST 800-53															•														1
RAMES (Risk Assessment method for embedded systems)																		•											**1**
Data mining-based framework																					•								**1**
Proposed ROSI framework																							•						1
Ontology-based Risk Management framework																									•				**1**
Distributed Agile Development Risk Management framework																										•			**1**
Trust-driven risk-aware access control framework																											•		**1**
Quantitative framework for business process-oriented IT RM																												•	**1**
Total	1	1	3	1	1	1	1	1	2	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

The most cited standard is ISO 31000:2009. It is the successor of Australian Standard for Risk Management (AS/NZS), 1999, and is a generic standard set that aims at harmonizing RM processes in existing and future standards but does not replace any of them [51]. The RM process is composed of the following seven activities [37]: Communication and Consultation; Establishing the Context; Risk Identification included on Risk Assessment; Risk Analysis included on Risk Assessment; Risk Evaluation included on Risk Assessment; Risk Treatment; Monitoring and Review.

ISO 31000:2009 is a process-oriented standard, but it is not structured or organised for rigorous process assessment neither does it specifically address IT organisations. This standard provides generic [57] high-level guidelines that help organisations with the implementation of the RM process into organisational processes but it does not clarify how the RM process should be integrated into the organisational processes and what techniques are necessary to perform RM activities [11].

The second most mentioned standard is PMBOK. This standard is the most popular standard for Project Management. PMBOK 5 is the most recent edition mentioned by the articles and proposes the following RM process composed of six activities [40]: RM Planning; Risk Identification; Qualitative Risk Analysis; Quantitative Risk Analysis; Risk Responses Planning; Risk Control.

Besides providing guidelines for managing projects and define project management concepts it also provides descriptions of tools and techniques [9].

Finally, the COSO ERM framework highlights the importance of considering risk in both the strategy-setting process and in driving performance [45]. The RM process proposed by this framework contains the following eight activities [54]: Internal Environment; Objective Setting; Event Identification; Risk

Assessment; Risk Response; Control Activities; Information and Communication; Monitoring.

According to COSO, ERM is *"...a process, ..., designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"* [59].

Many organisations that wish to implement or improve IT RM face difficulties in selecting an adequate approach aligned to their business challenges and market positioning. These difficulties relate to the fact that the already existing standards and frameworks describe RM in general, are extensive and unclear, some are not process-oriented, and others are not structured for rigorous risk assessment [57].

From Table 3.4, one can state that the scientific community is not fully satisfied with known standards/frameworks since 10 of the 23 standards/frameworks are frameworks created by the article's authors.

3.4.2 Synthesizing and connecting the IT RM's activities

During the article's analysis, a big diversity of IT RM activities was acknowledged. Moreover, it was discovered that many activities with different names have the same meaning. Table 3.5 shows activities, or combined activities from the same article, that mean the same as the top ten most proposed activities.

Table 3.5: Activities that means the same as the top 10 activities most mentioned in the articles from the final set

Top 10 most used IT RM activities	Number of articles	Activities that means the same
Risk Identification	22	Occurrence [47] Obstacle Identification [11] Resources and risks identification [50] Event identification [54, 56] Vulnerability and threat identification [14] Risks definition [59]
Risk Assessment	20	Risks identification and assessment [52] Risk Evaluation [43] Risks assessment and quantification [59]
Risk Analysis	12	Likelihood and impact determination [14]
Risk Treatment	9	Risk Prevention [33] Implementation of Protection Programs [50] Risk Control [42] Risk Mitigation [60]
Risk Response Planning	7	Identification of suitable tasks [52] Countermeasure analysis [14]
Context Establishment	6	Scope Establishment [11, 29] Context analysis [48] Goal refinement [11]
Risk Response	6	Impact; Control [47] Risk response strategies determination; Implementation [59]
RM Planning	5	Internal Environment; Objective Setting [54]
Risk Control	5	Risk Review [35]
Monitor and Control Risk	5	Risk Monitoring [29, 33] Effectiveness Measurement [50] Risk Monitoring and Review [51] Review of results and benefits of finished tasks [52] Monitoring [54, 56] Monitor, Consult & Management [55] Monitor and update [59]

With so many activities with different names but with the same meaning, the number of different activities identified decreases considerably.

Not all activities from the final set were identified as having the same meaning as other activities since many authors only mentioned the activity itself and do not describe it. As such, there is some lack of clarification of the activities that can compose the IT RM process stated by the articles.

Risk Identification will be considered one of the essential activities of IT RM since 33 articles, explicitly or implicitly, propose Risk identification and activities that have its meaning. This assumption is also supported by the fact that two of the most mentioned standards, namely ISO 31000:2009 and PMBOK 5, propose this activity.

From the 33 articles, 22 propose Risk Identification as not being part of Risk Assessment. This activity is usually proposed together with the activities Risk Assessment and Risk Analysis. From the 22 articles, 91% propose Risk Identification and Risk Assessment or Risk Analysis together. 64% of Risk Identification activities are accompanied with either Risk Treatment, Risk Response Planning and Risk Response activities. Additionally, from the 22 articles, 73% propose Risk Identification together with Monitor and Control Risk and Risk Control. Risk Identification is only put together with the activities Context Establishment and RM Planning in 45% of the 22 IT RM processes that propose Risk Identification as not belonging to Risk Assessment.

As mentioned above, Risk Identification is typically put together in the same process with Risk Assessment or Risk Analysis. These two last activities and the ones that mean the same as them are proposed in 36 articles. So, Risk Assessment and Risk Analysis are also considered essential activities of IT RM. As it can be observed in 3.5, Risk Analysis is proposed by 12 articles and 20 articles propose Risk Assessment, but it is important to notice that from the 20 articles that propose Risk Assessment, five include Risk Analysis as part of Risk Assessment. Now the challenge is to know which one is the most essential since both are never put together in the same IT RM process unless Risk Analysis is part of Risk Assessment. Considering that Risk Identification does not belong to Risk Assessment, as proposed by the majority of the articles, and ISO 31000:2009 and PMBOK 5 are the most popular standards and both include Risk Analysis. This activity will be considered as an essential part of IT RM.

From the 22 articles that propose Risk Identification, not counting with the ones that propose Risk Identification as part of Risk Assessment, three propose Risk Identification with Risk Treatment, seven with Risk Responses Planning and three with Risk Response. The standard ISO 31000:2009 proposes Risk Treatment, while PMBOK 5 proposes Risk Responses Planning, and COSO ERM proposes Risk Response. Since Risk Identification is mostly put together with Risk Responses Planning and this last activity is proposed by one of the most popular standards, it will be considered as one of the essential activities of IT RM. The problem is that the activity Risk Responses Planning can have two different meanings: determination of suitable actions to react to the identified risks; or the planning and adoption of strategies and responses for uncertainties to reduce risks [30, 46].

The challenge is then to understand if this activity includes both planning and adoption of responses to deal with risks or if it is only about the planning of those responses. According to PMBOK 5, Risk Responses Planning is the activity where strategies and actions are developed in order to reduce risks [63]. For that reason and for being one of the most popular standards regarding RM, this definition given by PMBOK 5 is the one that will be considered when describing Risk Responses Planning.

It is necessary to add to the IT RM process an activity that implements the plans and actions developed in Risk Responses Planning when required. From the seven articles that propose Risk Responses Planning, 57% of them put this activity together with Monitor and Control Risk and the remaining propose it together with Risk Education/Execution, Risk Control, that is an activity proposed by PMBOK 5, and Risk Evaluation.

Risk Evaluation is not even considered, since is about making the plans to treat risk and not their implementation. Risk Education/Execution is not considered since is an activity that is only proposed by one article from the final set. Regarding the two remaining activities, both are proposed by five different articles, but Monitor and Control Risk is usually together with Risk Responses Planning. Therefore, Monitor and Control Risk will be considered one of the essential activities of IT RM, since is the activity about the monitorization and control of the identified risks during the project, complementing Risk Responses Planning [30].

Finally, from the 22 articles that propose Risk Identification, not counting with the ones that propose Risk Identification as belonging to Risk Assessment, less than half put this activity together with Context Establishment and RM Planning. However, it is important to notice that two of the most popular standards from the final set of articles propose these activities, namely ISO 31000:2009 and PMBOK 5. The activity Context Establishment is important for Risk Identification, and it is about the definition of what the organisation aims to achieve as well as the definition of the internal and external factors that can help achieving those goals [16]. The objectives, scope and boundaries of the IT RM process should be defined, including IT RM activities' purpose and scope, and identify all the constraints that affect its scope. After identifying the constraints, the organisation should define the risk criteria that will be used throughout the process [64]. In summary, the organisation's context and IT RM process scope must be understood before risk identification. This activity is also one of the essential activities of IT RM.

The connections between the most popular IT RM activities proposed by the articles from the final set are established, but there are still some activities, that according to some authors and known standards and frameworks, are essential for the IT RM process.

According to ISO 31000:2009, an adequate IT RM process requires constant and structured communication with those affected by the organisation's operations, the activity responsible for that is Communication and Consultation, where communication has the aim of promoting risk awareness and understanding among relevant stakeholders, while consultation concerns with getting feedback and information to support decision-making. This activity will be considered an essential activity of IT RM [64].

So, the set of essential IT RM activities contains the following six activities: Communication and Consultation, Context Establishment, Risk Identification, Risk Analysis, Risk Responses Planning, and Monitor and Control Risk.

However, this set of activities is not based on the latest versions of ISO 31000 and PMBOK. To be aligned with the latest versions of the standards, the connections between ISO 31000:2009 and ISO 31000:2018, and PMBOK 5 and PMBOK 6 were studied and established, to check if the activities from both versions still match. After studying, and knowing that the literature about the latest versions is still scarce, it was chosen a process based on the standards' latest version since these are merely updated versions. For example, ISO 31000:2018 explains activities more simply and briefly, because it contains less RM jargon and less defined terms, and additionally expands some activities, not changing the basic structure and fundamentals of the activities' purpose and definition.

Monitor and Control Risk is an activity that means the same as Control Risks (PMBOK 5). In PMBOK 6, Control Risks is now named as Monitor Risks and they added one activity called Implement Risk Responses, emphasizing the importance of executing risk responses. Monitor and Control Risk is equivalent to Monitor Risks plus Implement Risk Responses.

ISO 31000:2018 proposes an activity named Risk Recording and Reporting, that is also an activity proposed by two articles of the final set. In this activity, the IT RM process and its outcomes should be documented and reported through adequate mechanisms. This activity is important since it aims at communicating IT RM activities and outcomes across the organisation; delivering information for the decision-making process; improving IT RM activities and supporting interaction between the stakeholders [13]. This activity will also be considered as one of the essential activities of IT RM.

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.

3.5 Conclusion

The SLR resulted in 44 articles. By analysing these articles, it was concluded that: (a) there is a big diversity of IT RM activities since 74 distinct activities were identified; (b) there is no consensus regarding which are the essential RM activities to deal with IT risks; (c) some researchers have based the IT RM process on already existing standards, being the most used ISO 31000, PMBOK, and COSO ERM; (d) other researchers created and proposed new frameworks due to limitations of the standards; and (e) IT RM has been a hot topic, which led to the design and revision of known standards and frameworks, and the constant development of new frameworks and solutions.

4

Design and Development

Contents

4.1 Introduction

By searching "risk management" AND "ontology" in the databases: (a) Web of Science Core Collection; (b) KCI-Korean Journal Database; (c) Russian Science Citation Index; (d) Current Contents Connect; (e) and SciELO Citation Index ; it was found 73 articles reaching as far back as 2019 (included). This number of articles is extremely small when considering that the solo interest subject "risk management" results in 55203 articles in the same databases. Moreover, the 73 articles concerning ontology are applied to multiple research areas and not as an abstract RM approach. Therefore, it is assumed that an ontology of RM is still an open research area and that domain-specific applications are preferred. IT RM is a well-defined domain-specific RM application where many of the known frameworks and standards demand a consensus ontological definition effort.

To overcome IT RM's complexity, it was decided to develop an ontology of IT RM, having as basis the results of the SLR. This ontology aims at simplifying and clarifying IT RM. The SLR conducted supplies definitions of the IT RM activities based on ISO 31000:2018 and PMBOK 6, as well as their relationships, dependencies, and who is responsible for what. As shown in Figure 4.1, the knowledge obtained from the SLR will serve as a basis for defining the essential model of IT RM using DEMO.

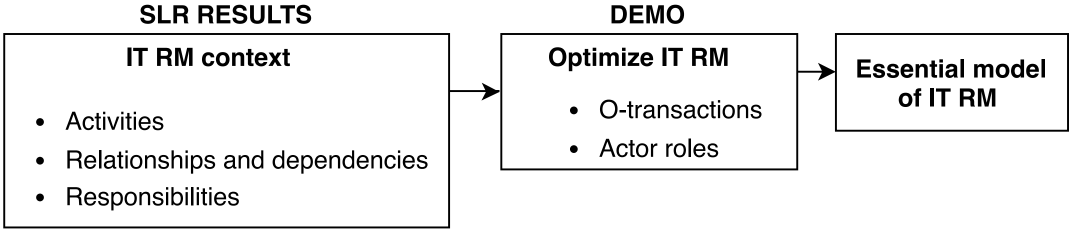

Figure 4.1: From a Systematic Literature Review to IT RM's essential model

This chapter outlines the extensive analysis of the IT RM activities that resulted from the SLR performed (Section 4.2), and the process of development of the essential model of IT RM (Section 4.3).

4.2 Analysis of the IT RM activities

Before defining the essential model of IT RM, first, it is necessary to analyse the definitions of the essential IT RM activities provided by the standards ISO 31000:2018 and PMBOK 6. The main purpose of this analysis is to identify the O-organisation transaction kind (O-transaction)s, where *Original P-acts* are carried out, and actor roles.

During the analysis of the IT RM activities' definitions, all realisation aspects (I-organisation transaction kind (I-transaction)s and D-organisation transaction kind (D-transaction)s of an organisation were ignored). I-transactions encompass *Informational P-acts*, while D-transactions comprehend *Documental P-acts*. Additionally, all implementation aspects are overlooked, i.e., the technologies that conduct the P-acts and C-acts, also the specific human beings that fulfil the actor roles were abstracted [2, 19].

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

The first IT RM activity **Communication and Consultation**, according to ISO 31000:2018, "Communication seeks to *promote awareness and understanding of risk and the means to respond to it*, whereas consultation involves *obtaining feedback and information* to support decision-making" [13]. In this definition, only I-transactions are present since these are about sharing and remembering facts.

As stated by ISO 31000:2018, **Scope, context and criteria** begins with "The organisation should *define the scope* of its risk management activities". When defining the scope, it is considered: (a) the objectives and decisions to be made; (b) the results expected from performing the process; (c) time, place, inclusions and exclusions; (d) adequate risk analysis tools and techniques; (e) resources necessary, responsibilities and documents to be stored; (f) and connections with other projects and processes [13].

Then, "The *context of the risk management process should be established* from the understanding of the external and internal environment in which the organisation operates..." [13].

Lastly, "...*define criteria* to evaluate the significance of risk and to support decision-making processes". To define risk criteria, one must consider: (a) the nature and type of uncertainties that can affect the results and objectives; (b) how risks' likelihood and impact will be defined and assessed; (c) time-related factors; (d) uniformity in the assessments; (e) how the risks level is to be decided; (f) how to consider combinations and sequences of numerous risks; (g) and the organisation's capacity [13].

In this activity, three O-transactions were determined, since they are about creating something new: (a) **T1 scope defining**, the actor role is **A1 scope definer** (initiator/executor); (b) **T2 context establishing**, the actor role is **A2 context establisher** (initiator/executor); and (c) **T3 risk criteria defining**, the actor role is **A3 risk criteria definer** (initiator/executor). These transactions access organisation's data.

The activity **Identify Risks**, according to PMBOK 6, is about "*identifying individual project risks as well as sources of overall project risk*...". PMBOK advises the involvement of experts, so that "*Individual project risks and sources of overall project risk can be identified*...", obtaining a list of those risks and respective sources. Experts are individuals or groups with specialised knowledge that take into account all aspects of risks and sources, based on their previous experience and areas of expertise [65].

Two O-transactions were identified in this activity, since these regard creating something new: **T4 risks identifying**, the actor role is **A4 risks identifier** (initiator/executor); **T5 individual risks and sources of overall activity risk identifying**, the actor roles are A4 (initiator) and **A5 subject matter proficient** (executor). During the process of carrying out T4, the corresponding T5 is initiated, hence is said that T5 is enclosed in T4, implying that A4 is the initiator of T5. In order to identify risks correctly, it is required to access information that resulted from T1, T2, T3 and also to access data from the organisation.

As it can be observed, the O-transactions and correspondent actor roles are identified by an id. There is no logic in assigning numbers to actor roles and transaction kinds, but there is a practical convention: the number of an actor role is the same as the number of the transaction kind of which it is the executor.

As stated by PMBOK 6, **Perform Qualitative Risk Analysis** includes "... *prioritizing individual project risks* for further analysis or action by *assessing their probability of occurrence* and *impact*..." [65]. Assessing the risks probability of occurrence and impact is subjective since these assessments are based on perceptions of risk by stakeholders. That is why these are considered O-transactions.

To successfully perform these assessments, it is performed a "*Risk data quality assessment* that evaluates the degree to which the data about...risks is accurate and reliable as a basis for qualitative risk analysis". This activity also "... *identifies a risk owner* for each risk who will take responsibility for planning an appropriate risk response and ensuring that it is implemented" [65]. Both actions are considered O-transactions since a judgement is being made regarding the data available and decisions about responsibilities are made.

Five O-transactions were identified: (a) **T6 risks priority assessment**, the actor role is **A6 risks analyser** (initiator/executor); (b) **T7 risks probability of occurrence assessment**, the actor roles are A6 (initiator) and **A7 risks probability of occurrence assessor** (executor); (c) **T8 risks impact assessment**, the actor roles are A6 (initiator) and **A8 risks impact assessor** (executor); (d) **T9 quality of risks information evaluating**, the actor roles are A7 and A8 (initiators), and **A9 risks information quality evaluator** (executor); and (e) **T10 risk owner identification**, the actor role is **A10 risks owners' identifier** (initiator/executor). The transaction kinds T7 and T8 are enclosed in T6, and T9 is enclosed in T7 and T8. To perform T6, T7 and T8, the executors need information from T4, and to identify the risk owner, it is necessary to access data that resulted of performing T1, T2 and access organisation data.

Perform Quantitative Risk Analysis, according to PMBOK 6, is the "... process of *numerically analysing the combined effect of identified...risks and other sources of uncertainty on overall project objectives*" [65]. It is an I-transaction since it is about computing, calculating and analysing data.

Plan Risk Responses, as stated by PMBOK 6, "Once risks have been identified, analysed and prioritised, *plans should be developed* by the nominated risk owner" to address every relevant risk. Moreover, "*The strategy or mix of strategies* most likely to be effective *should be selected* for each risk". In this activity, "...*actions are developed* to implement the agreed-upon risk response strategy ...". "*A contingency plan...can be developed* for implementation if the selected strategy turns out not to be fully effective or if an accepted risk occurs". "*Secondary risks should also be identified*" [65].

These definitions are O-transactions since they are about deriving something (developing) and deciding: (a) **T11 risk responses planning**, the actor role is **A11 risk owner** (initiator/executor); (b) **T12**

risk responses strategies selecting, the actor roles are A11 (initiator) and **A12 strategies selector** (executor); (c) **T13 actions developing**, the actor roles are A11 (initiator) and **A13 actions developer** (executor); (d) T4 risks identifying, the actor roles are A11 (initiator) and A4 (executor); and (e) **T14 contingency plan developing**, the actor roles are A11 (initiator) and **A14 contingency plan developer** (executor). The transaction kinds T12, T13 and T14 are enclosed in T11. To plan risk responses, it must be considered the risks' priority, so it is necessary to access the data that results from performing T6.

Regarding **Implement Risk Responses**, PMBOK 6 defends that "Expertise should be considered... to *validate or modify risk responses...and decide how to implement them* in the most efficient and effective manner". Moreover, "*Project documents that may be updated* as a result of carrying out this process", updating results of previous transactions [65].

Two O-transactions were identified. One regards decisions and the other is about updates that cannot be re-computed since these depend on new decisions: **T15 risks enhancing**, the actor role is **A15 risk responses implementer** (initiator/executor); **T16 risk responses implementation deciding**, the actor roles are A15 (initiator) and **A16 subject matter expert** (executor). The transaction kind 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** is about "...*monitoring the implementation of agreed-upon risk response plans*, ...*identifying and analysing new risks*, and *evaluating risk process effectiveness* throughout the project" [65].

Four O-transactions were identified, since they are about observing and creating something new: (a) **T17 implementation of risk responses monitoring**, the actor role is **A17 risk monitor** (initiator/executor); (b) **T18 risk management process effectiveness evaluating**, the actor roles are A17 (initiator) and **A18 RM process effectiveness evaluator** (executor); (c) T4 risks identifying, the actor roles are A17 (initiator) and A4 (executor); and (d) T6 risks priority assessment, the actor roles are A17 (initiator) and A6 (executor). The transactions T4, T6 and T18 are enclosed in T17. To monitor the implementation of risk responses, it is necessary to access T15.

Recording and Reporting, as stated by ISO 31000:2018, the RM process and its results "should be *documented* and *reported*..." [13]. Only I-transactions and D-transactions were identified.

4.3 IT RM Essential Model

Now it is possible to produce the essential model of IT RM, based on the analysis of this process's activities. The Plena tool (`https://www.teec2.nl/plenaen/plena-the-tool/`) was used to develop the aspect models that compose the essential model. This tool runs on the Enterprise Architect software. In this research work, it is used the terminology of DEMO version 3.7 since when developing this solution, version 4.0 was yet to be released, and Plena tool currently supports version 3.7.

4.3.1 Construction Model

The CM was the first model to be developed. This model is represented in a *Transaction Product Table (TPT)*, an *Organisation Construction Diagram (OCD)*, and a *Bank Contents Table (BCT)*.

As shown in Table 4.1, the TPT is a list of the transaction kinds, identified in Section 4.2, and corresponding product kinds. A TPT entry is: transaction kind id, transaction kind name, product kind id, product kind formulation [2].

Table 4.1: 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 OCD is exhibited in Figure 4.2. In this diagram, actor roles are represented by squares, whereas the O-transactions are represented by discs containing a red diamond.

The solid black lines without a black diamond, connecting actor roles and transaction kinds, are called *initiator links*. This means that actors in the actor role (e.g. A6 risks analyser) are an authorised initiator in transactions of the transaction kind (e.g. T7 *risks probability of occurrence assessment*). The solid black lines with a black diamond, connecting actor roles and transaction kinds, are called *executor links*. This implies that actors in the actor role (e.g. A7 risks probability of occurrence assessor) are an authorised executor in transactions of the transaction kind (e.g. T7 risks probability of occurrence assessment). The black dashed lines connecting actor roles and transaction kinds, which are now considered transaction banks, are called *information links*. This means that actors in the actor role (e.g. A8 risks impact assessor) have (reading) access to the contents (facts) of the corresponding transaction bank (e.g. T4 *risks identifying*) [2].

A *transaction bank* is the theoretical container of all facts that resulted from carrying out transaction kinds. The transaction bank AT1 comprises data about the organisation: its objectives, time, location,

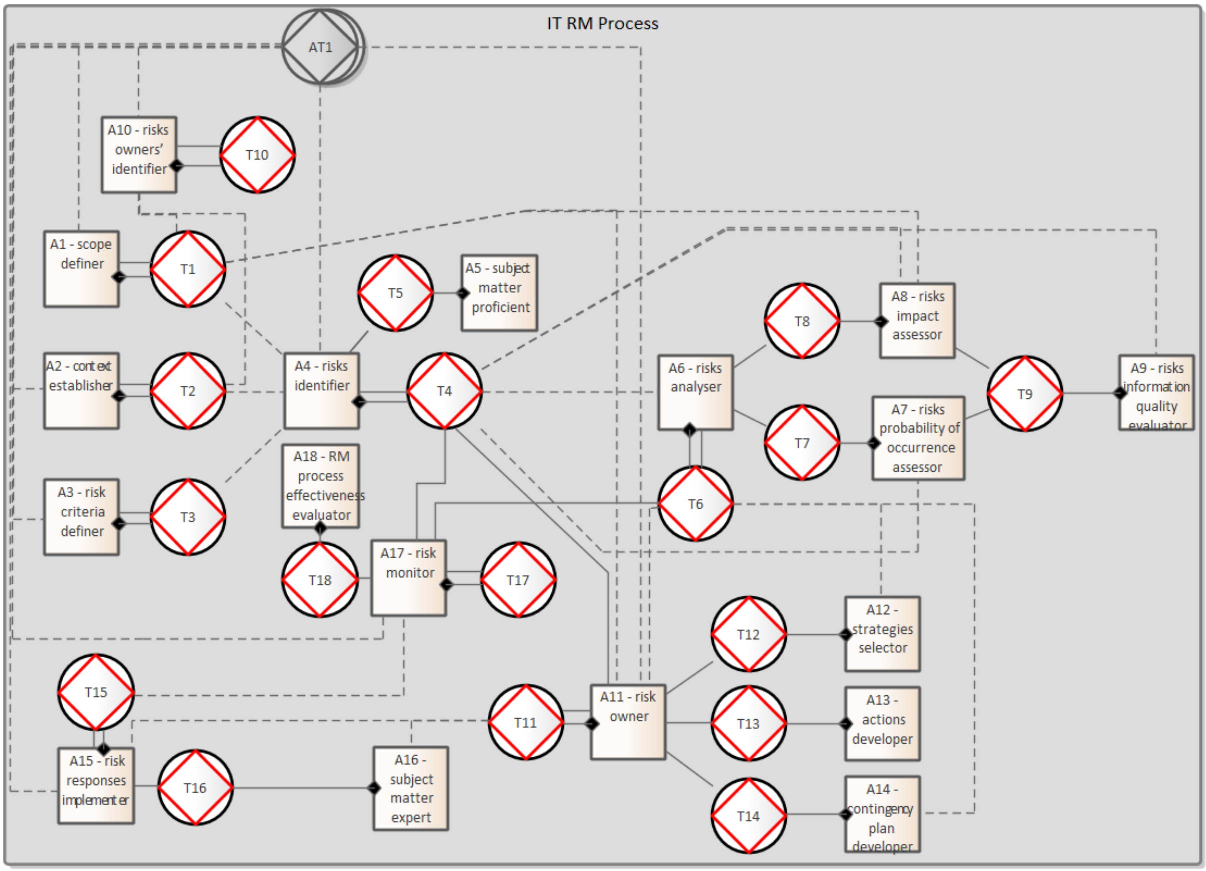
IT RM Process
AT1
A10 - risks owners' identifier
T10
A1 - scope definer
T1
T5
A5 - subject matter proficient
A2 - context establisher
T2
A4 - risks identifier
T4
A6 - risks analyser
T8
A8 - risks impact assessor
T9
A9 - risks information quality evaluator
T7
A7 - risks probability of occurrence assessor
A18 - RM process effectiveness evaluator
A3 - risk criteria definer
T3
T6
T18
A17 - risk monitor
T17
T12
A12 - strategies selector
T15
T11
A11 - risk owner
T13
A13 - actions developer
A15 - risk responses implementer
T16
A16 - subject matter expert
T14
A14 - contingency plan developer

Figure 4.2: Organisation Construction Diagram of IT RM

particular inclusions and exclusions, risk analysis tools and techniques, resources, responsibilities and records (such as the lessons learned register), relationships between projects and processes, organisation's environmental factors, obligations, among others [2].

As it can be observed in Figure 4.2, eight transactions are self-initiating, this means that the actor role is both the initiator and the executor of the transaction. This might not seem very realistic, but usually, management activities are self-control activities performed by the organisation since an external entity will not do it. The grey coloured box that contains all transaction kinds and actor roles represents the Scope of Interest and shows that the process of IT RM belongs to the organisation that implements it.

4.3.2 Process Model

The PM is a model of the (business) processes that take place as the effect of acts by actors. It is represented in a Process Structure Diagram (PSD). The PSD demonstrates the dependencies between the identified processes, in which way a transaction kind is enclosed in another one, and connects an organisation's CM and AM, regarding coordination [2].

Since the Plena tool creates a PSD for each transaction kind, it will only be shown the PSD of the transaction kind T6 *risks priority assessment*.

The discs of the transaction kind shapes are ’stretched’ horizontally in the PSD. A transaction proceeds in three phases: the order phase (left from the red diamond), the execution phase (the red diamond), and the result phase (right from the red diamond). The top part of the ’stretched’ disc correspond to the actions carried out by the initiator, while the bottom part regards the executor actions [2].

In the PSD, the terms “+rq”, “+pm”, “+ex” and “+ac” mean, respectively request, promise, execute and accept. Each one of them is an intention (disposition of the initiator concerning the product and the executor). For example, the intention of a ’promise’ is that the executor will bring the product in due time. The C-acts (+rq, +pm, +ac) and the P-act (+ex) are represented by white-filled boxes, while the pink-filled discs represent C-facts. Additionally, a PSD contains *response links* that are represented by solid black lines with an arrow, and *wait links* that are represented by dashed black lines [2].

As presented in Figure 4.3, is a self-initiation transaction that, in response to the status (T6/rq), the actor role A6 risks analyser carries out two acts: [T6/rq] and [T6/pm]. Then, in response to the status (T6/pm), the actor role A6 initiates T7 *risks probability of occurrence assessment* and T8 *risks impact assessment*. This implies that to assess the priority of risks, the actor role A6 first needs to ’request’ for the probability of occurrence of risks [T7/rq] and the impact of risks [T8/rq]. As soon as T7 and T8 reach the status of ’accept’ (T7/ac) and (T8/ac), T6 can be executed [T6/ex], which means that the actor role A6 can now assess the priority of risks. Notice that the brackets “(” and “)” represent C-facts and square brackets “[” and “]” represent C-acts or the P-act ’execute’.

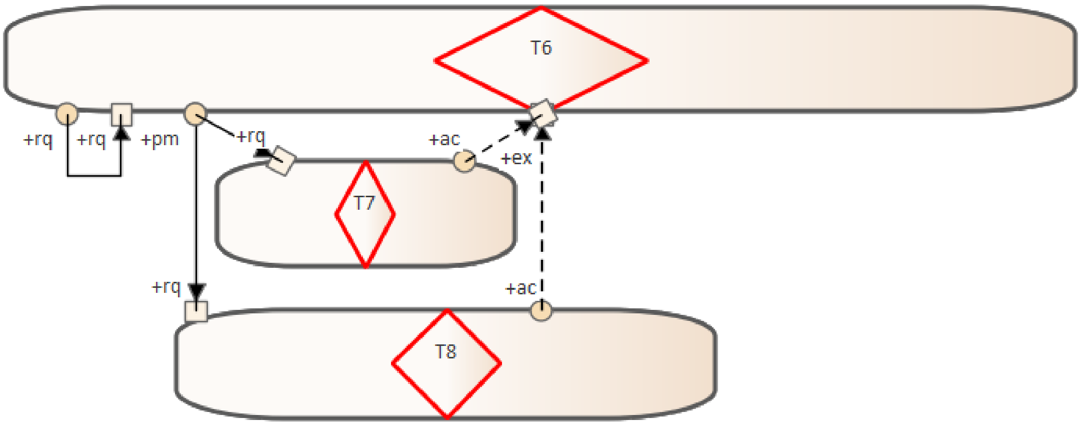

Figure 4.3: Process Structure Diagram of IT RM, regarding T6 risks priority assessment

4.3.3 Fact Model

The FM is represented in an Object Fact Diagram (OFD). It specifies which facts are relevant in the P-world. The FM connects an organisation’s CM and AM regarding production [2].

In the OFD, shown in Figure 4.4, the “roundangles” represent classes, for example, RISK. The red diamonds represent production event types, and these are identical to the product kinds presented in the TPT of the CM. So, the product kind identifier, for example, P7, is written inside the diamond. For example, the event type “the probability of occurrence of Risk is assessed” concerns the entity type Risk (or the entity class RISK) [2].

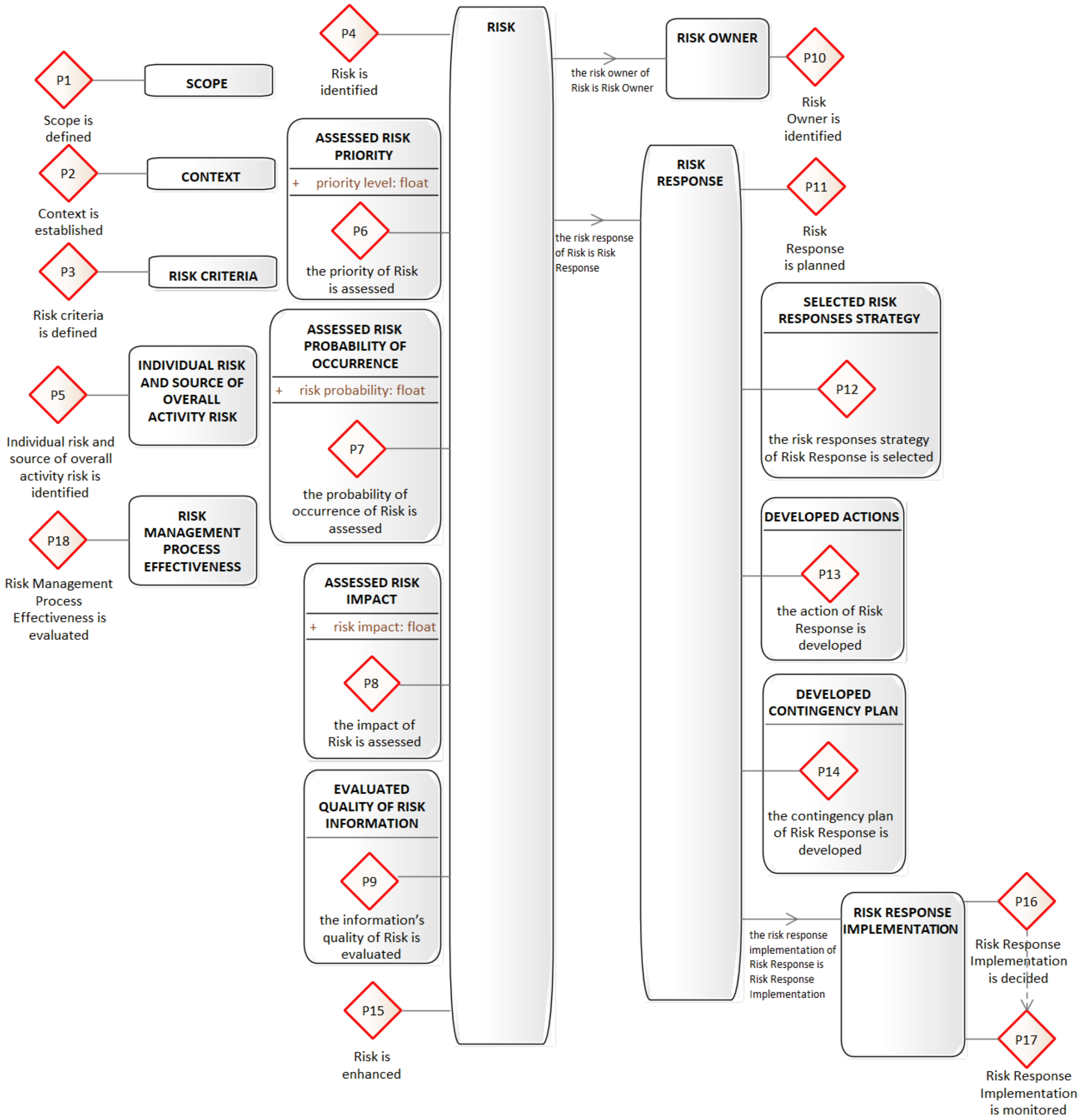
P1
Scope is defined
SCOPE
P2
Context is established
CONTEXT
P3
Risk criteria is defined
RISK CRITERIA
P5
Individual risk and source of overall activity risk is identified
INDIVIDUAL RISK AND SOURCE OF OVERALL ACTIVITY RISK
P18
Risk Management Process Effectiveness is evaluated
RISK MANAGEMENT PROCESS EFFECTIVENESS
P4
Risk is identified
ASSESSED RISK PRIORITY
+ priority level: float
P6
the priority of Risk is assessed
ASSESSED RISK PROBABILITY OF OCCURRENCE
+ risk probability: float
P7
the probability of occurrence of Risk is assessed
ASSESSED RISK IMPACT
+ risk impact: float
P8
the impact of Risk is assessed
EVALUATED QUALITY OF RISK INFORMATION
P9
the information's quality of Risk is evaluated
P15
Risk is enhanced
RISK
the risk owner of Risk is Risk Owner
the risk response of Risk is Risk Response
RISK OWNER
P10
Risk Owner is identified
RISK RESPONSE
P11
Risk Response is planned
SELECTED RISK RESPONSES STRATEGY
P12
the risk responses strategy of Risk Response is selected
DEVELOPED ACTIONS
P13
the action of Risk Response is developed
DEVELOPED CONTINGENCY PLAN
P14
the contingency plan of Risk Response is developed
the risk response implementation of Risk Response is Risk Response Implementation
RISK RESPONSE IMPLEMENTATION
P16
Risk Response Implementation is decided
P17
Risk Response Implementation is monitored

Figure 4.4: Object Fact Diagram of IT RM

The lines between classes represent property types, for instance, the property type “the risk owner of Risk is Risk Owner” is a function that maps RISK to RISK OWNER, implying that every risk has exactly one risk owner. The symbol “>” indicates that RISK is the domain of the function, and RISK RESPONSE is the range. Attribute types represent functions, where the domain is a class and the range is always a value class. These are inside the “roundagle” of the class that is its domain, and to their right, the name of the value class (function’s range) is written, for example, risk probability is an attribute type that has the class ASSESSED RISK PROBABILITY OF OCCURRENCE as its domain and the value class float as its range. [2].

According to PMBOK 6, descriptive terms (such as very high, high, medium, low, and very low) or numeric values can be used for risks probability of occurrence and impact. These values were considered as floats since the Plena tool only allowed one value class as the range of an attribute type.

The class RISK is the main concept of IT RM, and the domain of five product kinds, P4 Risk is identified, P6 the priority of Risk is assessed, P7 the probability of occurrence of Risk is assessed, P8 the impact of Risk is assessed and P9 the information’s quality of Risk is evaluated.

After defining the FM, it is possible to complete the CM by producing the BCT (Table 4.2). It shows the connections between all transaction kinds in the CM, that are now grouped according to the transaction banks in which they are stored, with the P-fact types in the FM. A BCT entry is: (transaction kind id | aggregate transaction kind id), (entity type name | product kind formulation | property kind formulation).

4.3.4 Action Model

The last model developed was the AM. For every internal actor role, the AM contains a set of *action rules*. The action rules are expressed in Action Rule Specifications (ARS) [2].

One transaction has multiple action rules, so as an example the ARS regarding T6 *risks priority assessment* is demonstrated in Figure 4.5.

Action rules are guidelines for actors when dealing with events (C-facts) that they must respond to. An action rule is split into three sequential parts: event part, assess part, and response part [2].

The *event part* specifies which event (or set of events) will be settled. It contains a when-clause, optionally complemented by a while-clause and a with-clause. In Figure 4.5, in the third action rule, the event to respond to is *risks priority assessment* being promised (T6/pm). Nevertheless, in this action rule, the when-clause contains a while-clause, which means that the actual settlement of the event (T6/pm) must wait until the events in the while-clause, *risks probability of occurrence assessment* being accepted (T7/ac) and *risks impact assessment* (T8/ac), has occurred. The events in the while-clause represent the wait links in the PM [2].

The *assess part* consists of a set of propositions whose truth value must be assessed. These propositions are grouped into the three validity claims: the claim to justice, the claim to sincerity, and the claim to truth. In this part, the event is assessed and it is checked if the actor has the authority to take the actor role A6 risks analyser (claim to justice). Notice that the assessment conditions are sometimes not

Table 4.2: Bank Contents Table of IT RM

bank	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
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 **is** enhanced
T16	RISK RESPONSE IMPLEMENTATION Risk Response Implementation **is** decided
T17	Risk Response Implementation **is** monitored
T18	RISK MANAGEMENT PROCESS EFFECTIVENESS Risk Management Process Effectiveness **is** evaluated
AT1	organisation **the** data **of** organisation

specific because the activity description is also sometimes not specific. After assessing the conditions, the response part begins [2].

The *response part* consists of the acts to be performed. The if-clause specifies what action to take if the actor considers complying with the conditions to be justifiable. In this case, after checking the intention of 'promise' through the validity claims, if the addressee considers that the intention is valid, the addressee will proceed with the event [T6/ex] followed by [T6/st] (then-clause). The addressee and performer of the event T6 being promised is the same actor role because T6 is a self-initiating transaction [2].

The acceptance of *risks probability of occurrence assessment* (or *risks impact assessment*) is the occurrence of the C-fact 'accept'. The actor role A6 risks analyser only executes *risks priority assessment* after accepting the outcomes of *risks impact assessment* and *risks probability of occurrence assessment*. The actor role A6 can only assess the priority of risk after having the probability of occurrence and impact of risks assessed. So, A6 accepts the result of T7 and T8. The dependency between the execution of T6 with the acceptance of T7 and T8 is demonstrated in the OCD (Figure 4.2).

4.4 Conclusion

The outcomes of the SLR served as input for developing an ontology of IT RM. DEMO was used to produce the ontology, because its models offer deep insight and overview of an organisation, as a result of the remarkable reduction of complexity that is enabled by being rooted in the EE theories [2]. Before defining the ontology, first, the IT RM activities resulted from the SLR were analysed to identify the O-transactions and the correspondent actor roles of the activities. In total, 18 O-transactions were identified. Then, the essential model of IT RM was developed (the complete essential model can be found in: https://github.com/Mariana-S-M-Rosa/Essential-Model-of-IT-RM-Thesis.git). First, the CM was produced then, the PM, the FM, and finally the AM.

ARS for T6 (1):

when	risks priority assessment **for** Risk is requested		(T6/rq)
	with **the** risk owner **of** Risk **is the** Risk Owner		
assess	*justice*:	**the** performer **of the** request **is the** risks analyser	
		the addressee **of the** request **is the** risks analyser	
	sincerity:	<no specific condition>	
	truth:	<no specific condition>	
if	*complying with* request *is considered justifiable*		
then	promise risks priority assessment **for** Risk		[T6/pm]
	with	**the** addressee **of the** promise **is the** risks analyser	

ARS for T6 (2):

when	risks priority assessment **for** Risk is promised		(T6/pm)
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	request	risks probability of occurrence assessment **for** Risk	[T7/rq]
	with	**the** addressee **of the** request **is the** risks probability of occurrence	
	assessor		
	request	risks impact assessment **for** Risk	[T8/rq]
	with	**the** addressee **of the** request **is the** risks impact assessor	

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	

ARS for T6 (4):

when	risks priority assessment **for** Risk is stated		(T6/st)
	with **the** priority level **of** Risk **is some** float		
assess	*justice*:	**the** performer **of the** statement **is the** risks analyser	
		the addressee **of the** statement **is the** risks analyser	
	sincerity:	<no specific condition>	
	truth:	<no specific condition>	
if	*complying with* statement *is considered justifiable*		
then	accept	risks priority assessment **for** Risk	[T6/ac]
	with	**the** addressee **is the** risks analyser	

Figure 4.5: Action Rule Specification for T6 risks priority assessment

5

Demonstration

Contents

5.1 Introduction

According to EO, an organisation is “a network of actors who carry out transactions in cooperation”. Actors are responsible for the organisation’s operation (transactions), and the results of those transactions are products [2]. Therefore, the demonstration of the proposal includes the identification of transaction kinds and corresponding P-fact types of the IT RM ontology in the IT RM processes proposed by selected case studies, and the identification of gaps between the ontology and those case studies. Later, in Chapter 6, those gaps will be analysed in detail.

A BCT for each IT RM process proposed by the case studies was built to check if the transaction kinds and P-fact types of the IT RM ontology are present in those processes. The BCT is a list of the P-fact types, whose instances are created or used by the actor roles in transactions of the identified transaction kinds (now perceived as transaction banks). They are grouped based on the transaction banks in which they are stored [2].

To select proper IT case studies, it was checked if: (a) the case study contained factors, such as organisational structure (centralized or not), culture, strategy, maturity, regional differences, industry, size, trust, and ethic [66]; (b) the authors of the case study followed Yin guidelines [67] since if a case study does not follow any methodological guidelines, the probability of leaving out relevant information is high; (c) the case study is important, by verifying the journal or conference in which the article was published, the classification of the journal or conference, and the number of citations; (d) the case study was recently published; and (e) the description of the RM process proposed to deal with IT risks is detailed.

This chapter outlines the analysis and the results of the demonstration of each case study selected (Section 5.2, Section 5.3 and Section 5.4).

5.2 Case Study 1

Table 5.1 shows the analysis performed on the first case study selected to demonstrate the proposal, that is “An empirical study on the implementation and evaluation of a goal-driven software development risk management model” [11].

The first case study proposes the Goal-driven Software Development Risk Management Model (GSRM), a framework that supports the assessment and management of risks based on the KAOS goal modelling language. The authors opt for an IT RM process based on goal modelling since “goals and risks are complementary entities of a software project”.

This framework consists of four layers to support software development risk management: *goal layer* (focuses on the goals that contribute to the project success), *obstacle layer* (identifies and provides an overview of the potential risk factors that are considered obstacles which reduce the ability to achieve

Table 5.1: Analysis of the case study 1

Case Study Variables	**An empirical study on the implementation and evaluation of a goal-driven software development risk management model**
Year	2014
Journal	Information and Software Technology
Classification	Q1
Citations	54
Guidelines Yin	Yes
Organisational structure	Not present
Culture	Not present
Strategy	IT for efficiency (automate day-to-day ministry operational activities)
Maturity	Not present
Region	Bangladesh
Industry	Software Industry (Software development, global IT support, and consultancy)
Size	Not present
Trust	Not present
Ethic	Not present
IT RM process	(1) Initialise goal-driven risk management, (2) Identify and model goals, (3) Identify and model obstacles, (4) Assess risks, and (5) Treat and monitor risks
Detailed	Yes

goals and create problems in the project), *assessment layer* (establishes the causal relationship model between risk factors and related risk events, estimates the risk level of risks taking into consideration the risk events' likelihood and severity of impact on goals), and *treatment layer* (focuses on controlling risks, monitoring the effectiveness of the implemented control actions throughout the project life cycle, and identifying any new risks).

The GSRM contains activities that describe all the tasks and steps needed for goal-driven RM.

The first activity is *Initialise goal-driven risk management*. This activity includes determining the riskiness nature of the project, identify the main factors for the high risk project, define the RM scope, and establish the RM context. The GSRM adopts the context concept of ISO 31000:2009 and follows the standard to establish the RM context within the process. In this activity, three transaction kinds and correspondent P-fact types that are present in the IT RM ontology were identified. The transaction kinds are *T1 scope defining*, *T2 context establishing*, and *T3 risk criteria defining*.

The next activity is *Identify and model goals*, it involves the identification and categorisation of goals and the refinement of those goals that results in the construction of a goal model. This activity does not contain any transaction kind and P-fact type of the essential model of IT RM.

The following activity is *Identify and model obstacles*, it focuses on the identification and modelling of obstacles. This activity includes one transaction kind and correspondent P-fact type that is present in the IT RM ontology, that is *T4 risks identifying*.

The next activity is *Assess risks*, it involves assessing risks by estimating their risk level and priority. First, a causal relationship model is defined so that one focus only on estimating the risk level of relevant risk events instead of considering all risk factors. Risk estimation takes into account risk event likelihood and risk impact. Then, the risks are prioritised into three scales ("very important", "important", and "less important"), so that risks with high priority get immediate attention. In this activity, three transaction kinds and their P-fact types were detected, these are *T6 risks priority assessment*, *T7 risks probability of occurrence assessment*, and *T8 risks impact assessment*. The case study does not specify the values of risk probability and impact, so these are considered as 'String' because priority level is a 'String' and PMBOK 6 states that these fields can either be descriptive terms or numeric values [65].

The last activity is *Treat and monitor risks*. To treat risks, this activity must be planned and matched with the RM scope. it involves identifying the possible control actions and selecting the most cost effective one so that goals could be achieved. After the implementation of the selected control actions, this activity monitors the effectiveness of control actions, and identifies any new risks throughout the project. This activity includes five transaction kinds and their corresponding P-fact types, these are *T11 risk responses planning*, *T12 risk responses strategies selecting*, *T13 actions developing*, *T17 implementation of risk responses monitoring*, and *T18 risk management process effectiveness evaluating*.

All transaction kinds and corresponding P-fact types identified are presented in the BCT in Table 5.2.

Table 5.2: Bank Contents Table of the case study 1

bank	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 response **of** Risk **is** Risk Response
T6	**the** priority **of** Risk **is** assessed **the** priority level **of** Risk **is** String
T7	**the** probability of occurrence **of** Risk **is** assessed **the** risk probability **of** Risk **is** String
T8	**the** impact **of** Risk **is** assessed **the** risk impact **of** Risk **is** String
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
T17	Risk Response Implementation **is** monitored
T18	RISK MANAGEMENT PROCESS EFFECTIVENESS Risk Management Process Effectiveness **is** evaluated

As it can be observed in Table 5.2, the IT RM process proposed by the case study does not include six transaction kinds that are present in the IT RM ontology, specifically *T5 individual risks and sources of overall activity risk identifying*, *T9 quality of risks information evaluating*, *T10 risk owner identification*, *T14 contingency plan developing*, *T15 risks enhancing*, and *T16 risk responses implementation deciding*.

5.3 Case Study 2

Table 5.3 shows the analysis carried out on the second case study selected to demonstrate the proposal, which is “Introducing OSSF: A framework for online service cybersecurity risk management” [52].

Table 5.3: Analysis of the case study 2

Case Study **Variables**	**Introducing OSSF: A framework for online service cybersecurity risk management**
Year	2017
Journal	Computers & Security
Classification	Q1
Citations	28
Guidelines Yin	Yes
Organisational structure	Not present
Culture	Not present
Strategy	Not present
Maturity	Not present
Region	Not present
Industry	Online Service Industry (Online service provider and consumer)
Size	"large enterprise"
Trust	Not present
Ethic	Not present
IT RM process	(1) General threat scenarios identification, (2) Specific threats identification, (3) Risks identification and assessment, (4) Risk treatment, (5) Identification of suitable tasks, (6) Tasks prioritization, (7) Tasks execution, and (8) Review of results and benefits of finished tasks
Detailed	Yes

This case study proposes a new framework to support online services security risk management activities, called Online Services Security Framework (OSSF). This framework incorporates a Threat model, a Risk model, and a Meta model. The Meta model describes the framework, and the Threat model and Risk model are autonomous parts of the Meta model.

The Threat model’s purpose is to promote awareness and support the identification of all possible threat scenarios that might occur in a particular online service context. This model is able to identify, categorise, and describe threats.

The Risk model’s purpose is to identify, assess, and treat risks. It is composed of five elements: (a) the *threat scenario component* is based on the Threat model and aims at supporting risk identification by describing the threats related to risks; (b) the *risk assessment component* has the purpose of determining a risk’s severity based on a qualitative risk analysis methodology defined in ISO/International Electrotechnical Commission (IEC) 27005:2011; (c) the *risk treatment component* describes the risk treatment options proposed by ISO/IEC 27005:2011, the goals of security controls applied within risk treatment and the nature of the security controls; (d) the *risk classification component* is a classification scheme for risks; and (e) the RM process .

The RM process is proposed in accordance with the standard ISO/IEC 27005:2011. This process contains eight activities that are carried out successively.

The first activity is *General threat scenarios identification*. In this activity, based on the Threat model, general threat scenarios are chosen, which can arise in a specific online service context. This activity does not contain any transaction kind and P-fact type that is present in the IT RM's ontology.

The following activity is *Specific threats identification*, taking into account the list of general threat scenarios, appropriate threat categories are selected, and the current online service context is considered by more detailed threats' description. This activity does not include any transaction kind and P-fact type that is present in the essential model of IT RM.

The next activity is *Risks identification and assessment*. It involves the identification and description of risks that arise from threats, the assessment of risks, and considers the vulnerabilities of the affected assets. Regarding this activity, four transaction kinds and their P-fact types were detected, these are *T4 risks identifying*, *T6 risks priority assessment*, *T7 risks probability of occurrence assessment*, and *T8 risks impact assessment*. The case study states that, when assessing risk, the risk score is the sum of likelihood and impact values, that are expressed as numbers, so the priority level, probability, and impact of risk are considered as integers.

Risk Treatment is the next activity. It is where the decision regarding adequate risk treatment options (risk modification, retention, avoidance, and sharing) is made. This activity includes one transaction kind and corresponding P-fact type, that is *T12 risk responses strategies selecting*.

The next activity is *Identification of suitable tasks*, focuses on the identification of tasks to implement the selected risk treatment. In this activity, the transaction kind *T13 actions developing* and corresponding P-fact types were identified.

Tasks prioritization is about prioritising the tasks according to the related risk score and ordering them. After prioritising tasks, these are scheduled. This activity does not contain any transaction kind and P-fact type.

Tasks execution is the next activity. It focuses on the performance of the scheduled tasks and monitors their status. This activity includes one transaction kind and corresponding P-fact type that is present in the IT RM ontology that is *T17 implementation of risk responses monitoring*.

The last activity is *Review of results and benefits of finished tasks*. This activity focuses on checking whether and how much the results of performing the tasks contributed to reducing the relevant risk scores. This activity includes one transaction kind and its corresponding P-fact type that is *T18 risk management process effectiveness evaluating*.

All transaction kinds and corresponding P-fact types of the essential model identified in the IT RM process proposed by the case study are exhibited in the BCT in Table 5.4.

Table 5.4 shows that this case study proposes a process that does not include ten transaction kinds of IT RM's essential model, namely *T1 scope defining*, *T2 context establishing*, *T3 risk criteria defining*, and *T11 risk responses planning*, plus the ones that were not also present in the first case study.

Table 5.4: Bank Contents Table of the case study 2

bank	facts
T4	RISK Risk **is** identified **the** risk response **of** Risk **is** Risk Response
T6	**the** priority **of** Risk **is** assessed **the** priority level **of** Risk **is** Int
T7	**the** probability of occurrence **of** Risk **is** assessed **the** risk probability **of** Risk **is** Int
T8	**the** impact **of** Risk **is** assessed **the** risk impact **of** Risk **is** Int
T12	RISK RESPONSE **the** risk responses strategy **of** Risk Response **is** selected
T13	**the** action **of** Risk Response **is** developed
T17	Risk Response Implementation **is** monitored
T18	RISK MANAGEMENT PROCESS EFFECTIVENESS Risk Management Process Effectiveness **is** evaluated

5.4 Case Study 3

At the final stage of this research work, an analysis was performed of the “STAYAWAY COVID” system since it is the main focus of a subsequent research work based on this dissertation. This analysis is not as extensive as the previous two case studies, and it does not explicitly state the activities that are part of the IT RM process.

“STAYAWAY COVID” is a system created to trace the spread of COVID-19 through the voluntary use of an application for personal mobile devices. The main purpose of this application is to alert its user in case of proximity with other users of the application who were diagnosed with COVID-19. This system involves processing personal data, so the creators must evaluate the impact on data protection, according to article 35 of General Data Protection Regulation (GDPR).

The evaluation of the impact on data protection is documented in a report named “Avaliação de Impacto sobre a Proteção de Dados - Sistema STAYAWAY COVID” by Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC) and Instituto de Saúde Pública da Universidade do Porto (ISPUP). This report includes an analysis of the risks and vulnerabilities regarding the system’s data protection. So, this report was analysed to identify the gaps between the IT RM ontology and the IT RM process applied by the report’s authors.

To assess the impact on data protection, the authors followed some methodologies, including a set of standards, being one of them ISO 31000:2009. This standard was one of the standards that formed the basis of the essential IT RM process. However, this work adopts the latest version of this standard (ISO 31000:2018). Still, many compatibilities between the ontology and the process implemented in the

“STAYAWAY COVID” system were found.

By applying an IT RM process based on ISO 31000:2009, this case study includes all transaction kinds related to the activity *Scope, context and criteria*. These are *T1 scope defining*, *T2 context establishing*, and *T3 risk criteria defining*. First, the purpose of this process is to consider the vulnerabilities of this system regarding data protection and adopt proper mitigation actions for risks, mostly related to the possible re-identification of users that have been diagnosed with COVID-19. Then, risk sources are identified, and the issues to be considered during IT RM are determined. The assessment of risks' probability and impact is then defined to ensure consistency on its usage by following a methodology. Lastly, it is established the assessment of risks' severity and determined the type and nature of risks to be considered.

The main focus of the IT RM process applied is on risks related to the re-identification of users. However, before mitigating these risks, they have to be identified (*T4 risks identifying*). One of the risks identified is the information regarding users being found or deducted, for example, people's movements.

To analyse risks, the authors assess risks' probability and impact as 'String'. So, the transaction kinds *T7 risks probability of occurrence assessment* and *T8 risks impact assessment* are present in this case study.

Regarding treating risks, this case study includes *T11 risk responses planning*, *T12 risk responses strategies selecting*, and *T13 actions developing*. The authors plan risk controls, decide if a risk must be avoided, mitigated, or accepted, if there is no solution, and determine actions to control risks.

Finally, the authors state that the implementation of control risks and their effectiveness must be verified. This statement corresponds to both *T17 implementation of risk responses monitoring* and *T18 risk management process effectiveness evaluating*.

This case study does not lack one transaction kind that the other two case studies do lack, that is *T16 risk responses implementation deciding* since strategies suggested by Centro Nacional de Cibersegurança (CNCS) and recommended by Comissão Nacional de Proteção de Dados (CNPD) are taken into account when deciding the implementation of planned mitigation strategies for risks.

As it can be observed in Table 5.5, when analysing the process applied in this case study, a total of twelve transaction kinds that are present in the IT RM ontology were identified, so only six transaction kinds are not included in the process implemented in the case study.

The missing transaction kinds are: (a) *T5 individual risks and sources of overall activity risk identifying*; (b) *T6 risks priority assessment*; (c) *T9 quality of risks information evaluating*; (d) *T10 risks owner identification*; (e) *T14 contingency plan developing*; (f) and *T15 risks enhancing*.

Table 5.5: Bank Contents Table of the case study 3

bank	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 response **of** Risk **is** Risk Response
T7	**the** probability of occurrence **of** Risk **is** assessed **the** risk probability **of** Risk **is** String
T8	**the** impact **of** Risk **is** assessed **the** risk impact **of** Risk **is** String
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
T16	RISK RESPONSE IMPLEMENTATION Risk Response Implementation **is** decided
T17	Risk Response Implementation **is** monitored
T18	RISK MANAGEMENT PROCESS EFFECTIVENESS Risk Management Process Effectiveness **is** evaluated

5.5 Conclusion

To demonstrate the proposal, it was carefully analysed a set of case studies to choose adequate ones to apply the artifact produced. The first two case studies lack some information regarding the variables considered during the analysis. However, they are very detailed regarding the IT RM process proposed, which allowed the identification of the transaction kinds and P-fact types in the process's activities.

The authors of the first case study are not satisfied with the current RM frameworks and standards, because these have limitations and do not provide a detailed guideline and clear evidence on how to integrate RM activities into the project [11]. So, they propose the GSRM framework that comprises an IT RM process composed of five activities. During the analysis of these activities, twelve transaction kinds and corresponding P-fact types were identified, which are present in the essential model of IT RM.

The second case study proposes a novel framework specific for online service cybersecurity RM since no such framework exists [52]. This framework proposes an IT RM process in accordance to ISO 27005:2011, comprising eight IT RM activities. When analysing these activities, eight transaction kinds and corresponding P-fact types that are also part of the IT RM ontology were identified.

By comparing the BCTs of both processes (Tables 5.2 and 5.4), it can be stated that the IT RM process proposed by the second case study has more gaps than the first one regarding the transaction kinds and P-fact types of the essential model of IT RM.

The third case study does not propose a new framework like the previous two case studies but follows some methodologies being one of them ISO 31000:2009. During the analysis of the process applied, twelve transaction kinds that are present in the ontology of IT RM were identified.

6

Evaluation

Contents

6.1 Introduction

This chapter presents the evaluation process used to validate the proposal, which is to justify the implication of the lack of transaction kinds and P-fact types in the IT RM processes proposed by the case studies. If the case study does not contain transaction kinds and corresponding P-fact types in their process, are these not relevant for the case study or for the ontology?

Additionally, this chapter explains the implication of the activities in excess proposed by the case studies. Are these activities essential and should be part of the ontology of IT RM?

This chapter outlines the analysis of the implication of the gaps (lack or excess of elements) identified in each case study (Section 6.2, Section 6.3 and Section 6.4).

6.2 Case Study 1

The framework proposed by “An empirical study on the implementation and evaluation of a goal-driven software development risk management model” [11], defines a set of IT RM activities and enables the identification and rationalisation of the risk factors, events, and control actions regarding the goals. Besides focusing on risks, this framework focuses on goals, which are “the factors that contribute effectively to complete the project activities and directly link to the project success”. Goals are significant since they detail what is necessary to reach project success and who is responsible for achieving the goal.

Since the framework focuses on goals, it includes an activity for goals, that is *Identify and model goals*. This activity “...mainly identifies and categorises goals and refines high level goals to provide more concrete meaning in terms of their contribution to the project success”. This activity results in an artifact that is goal detail, which initiates following risk assessment and management activities. Goals can either be “complete project within estimated budget and schedule”, or “complete user’s training”, among others. When identifying risks, if the raw list of risks is extensive, it can be refined by following the identified goals.

This activity is not present in the IT RM ontology. However, the standards’ activities from which the transaction kinds of the IT RM ontology were identified take into consideration the organisation/process/project’s goals. Therefore, both processes take into consideration goals since risks can affect the achievement of these. But, is it really necessary to build a goal model?

In the case study, modelling goals does not influence the analysis of risks. The goal model, together with the risk model, might facilitate the communication of risk information. However, if a project focuses on a large number of goals, more effort will be required in analysing the goals and constructing goal-risk and causal relationship models, resulting in an increase of the process’s complexity. Also, by refining the list of identified risks, the managers do not consider or keep track of all risks that might affect the project’s success.

The main objectives of an RM process is “to increase the probability and/or impact of positive risks and to decrease the probability and/or impact of negative risks, in order to optimize the chances of project success” [65]. So, it is not essential to focus and detail that much on goals.

Assess risk is an activity that is not entirely part of the essential model of IT RM since, besides assessing risks, it involves the definition of the causal relationship model between risk factors and consequent risk events. The causal relationship model “allows us to focus on the relevant risk events for the risk level estimation, rather than considering all raw risk factors”.

PMBOK 6 proposes the activity *Perform Qualitative Risk Analysis*, which contains the transaction kinds T6, T7, T8, T9, and T10 of the IT RM ontology. This activity does not include the definition of a causal relationship model. If there are risks with low probability and impact, these must not be ignored. According to PMBOK 6, risks with low probability and impact can be included in the risk register for future monitoring since their relevance might change over time [65].

The purpose of the causal relationship model, as mentioned previously, is to focus only on relevant risks, but risks change and must always be considered. It is not necessary to construct a causal relationship model to analyse risks. This activity proposed by the case study looks like a filter that leaves some risks out. PMBOK 6 defends that “Risk responses should be appropriate for the significance of the risk, cost-effective in meeting the challenge, realistic within the project context...” [65].

Regarding the transaction kinds and P-fact types of the IT RM ontology, the case study lacks six transaction kinds.

The case study does not include the transaction kind *T5 individual risks and sources of overall activity risk identifying*. According to PMBOK 6, the expertise from individuals or groups with specialized knowledge of similar projects or business areas should be taken into account when identifying risks. These experts are invited to consider all aspects of project risks and sources based on their previous experience and areas of expertise. The activity *Identify Risks* is vital for any project’s success since unidentified risks are threats to project success.

The role of the expert is necessary during the identification of risks because the experts’ opinions may reduce the impact of risks and may help to make unbiased and accurate decisions [65].

T9 quality of risks information evaluating is another transaction kind that is not present in the IT RM process of the case study. According to PMBOK 6, assessing the quality of the data regarding risks helps to clarify the assessment of each risk’s relevance. The purpose of this transaction is to evaluate the degree to which the data about each risk is correct and reliable as a basis to *Perform Qualitative Risk Analysis* or, regarding the case study, to perform *Assess risk*. The utilisation of low-quality risk data may lead to a qualitative risk analysis that is worthless. If data quality is inappropriate, it may be required to gather better data [65].

PMBOK 6 states that *T10 risks owner identification* involves the identification of a risk owner for each risk. The risk owner is an individual responsible for monitoring risk, planning appropriate risk responses, and ensuring that the risk response is implemented. Moreover, these individuals may help in evaluating their risks during risk analysis. Only the most significant risks need a risk owner and risk response plan. The risk owner must have the ability to manage the risk and have the knowledge, resources, and authority to deal with the risk. Selecting the risk owner usually involves considering the source of risk and identifying the person who fits better to understand and implement what needs to be done [65].

It is crucial to select a risk owner since the risk's management is ensured, and in case of risk occurrence, one knows who is responsible for what and easily find out what went wrong.

The treatment layer of the IT RM process of the case study includes an individual who is responsible for implementing the selected control actions to manage risks. So, the case study partially contains the transaction kind T10.

T14 contingency plan developing is another transaction kind that is missing in the case study's process. PMBOK 6 defends the development of a contingency plan for implementation if the selected countermeasure proves not to be fully effective or if an accepted risk occurs. One might think that it is not necessary to develop a contingency plan if it might never be implemented. However, that is not true. When a risk has been triggered, a contingency plan is carried out. The purpose of the plan is to reduce the negative effects of risk when it occurs. Without the plan in place, the full impact of risk could severely affect the project [65].

The contingency plan is the last line of defense against the risk. It is better to have the contingency ready for implementation than to have to develop one as the risk is taking its toll [65].

The IT RM ontology contains *T15 risks enhancing*, a transaction kind that is not present in the case study. This transaction kind regards proposing changes to risk documents, such as the risk register, report, and to the lessons learned register, that resulted and are updated/modified in other transaction kinds. When implementing risk responses, new risk information will arise, and risk response information might change. The risk register and the risk report may be updated to reflect alterations to the risk response selected that are subsequently made as a result of implementing risk responses [65].

It is important to keep risk documents updated since these influence heavily the RM process. For example, the risk register records all identified risks along with their priority level and the actions and steps to be taken to mitigate the risk. The risk register is considered by managers as a management tool for monitoring the RM processes within the project [65].

T16 risk responses implementation deciding is one of the transaction kinds not included in the IT RM process of the case study. PMBOK 6 defends that experts' knowledge must be considered to validate or change risk responses if required, and decide how to implement them efficiently and effectively. The best scenario would be choosing an individual with expertise as the risk owner since is who is responsible for planning the risk response [65].

Table 6.1 summarises the gaps (lack or excess of elements) identified in the case study and indicates if the case study is completely lacking/exceeding those elements.

Table 6.1: Lack and excess of elements in case study 1

Excess	
Activities	*Level*
Identify and model goals	●
Assess risk	◐
Lack	
Transaction kinds	*Level*
T5 individual risks and sources of overall activity risk identifying	●
T9 quality of risks information evaluating	●
T10 risk owner identification	◐
T14 contingency plan developing	●
T15 risks enhancing	●
T16 risk responses implementation deciding	●

6.3 Case Study 2

The framework proposed by "Introducing OSSF: A framework for online service cybersecurity risk management" [52], includes an IT RM process based on ISO/IEC 27005:2011. This standard provides guidelines for information security RM and assists in the satisfactory implementation of information security based on an RM approach. Unlike ISO 31000, instead of considering all types of risks, ISO/IEC 27005:2011 is specific for information security risks [68].

A threat, as stated by the case study, is the "potential cause of an unwanted incident, which may result in harm to a system or organisation". According to ISO 31000:2018, a risk is the "effect of uncertainty on objectives". An effect is a variation from the expected, and it can be either positive, negative, or both, and can address, produce, or result in opportunities and threats [13].

The essential model of IT RM does not contain any transaction kinds or P-fact types regarding the identification of threats, unlike this case study that proposes two activities which focus on threats, namely *General threat scenarios identification* and *Specific threats identification*. The purpose of these two activities is to support risk identification through threat identification.

In the IT RM ontology, the transaction kinds that support the ones related to the identification of risk are the transactions related to the activity *Scope, Context and Criteria*. PMBOK 6 states that some techniques used to analyse data to identify risks allow the identification of threats. But threat identification is not necessary to identify risks, according to both PMBOK and ISO 31000 [13, 65].

One of the outputs of *Identify risks*, according to PMBOK 6, is the Risk Report that includes information regarding the identified risks, such as the number of identified threats and opportunities, among others. When performing qualitative risk analysis, one finds out if a risk imposes a threat or an opportunity. A risk with a negative impact is considered a threat (delay, additional cost, and performance shortfall) [65]. So, the essential process of IT RM partially includes *Specific threats identification*.

The activity *Tasks prioritization* is not present in the essential model of IT RM. This activity helps to ensure that mitigation tasks associated with high scored level risks will be performed without delays. According to PMBOK 6, when selecting the risk response strategy and developing actions to implement the agreed-upon risk response strategy, the risk priority level can help to guide the selection of appropriate risk responses. For example, high-priority level threats or opportunities may need priority action and highly proactive response strategies. One of the inputs of this activity is a document named Project schedule, where "the schedule is used to determine how agreed-upon risk responses will be scheduled alongside other project activities" [65].

By analysing the description of both activities, *Tasks prioritization* is implicit in *Plan Risk Response* of PMBOK 6 since the tasks prioritisation done in the case study is equivalent to attribute actions and response strategies to risks according to their priority level in the IT RM ontology.

Regarding the transaction kinds and P-fact types of the IT RM ontology, the case study lacks ten transaction kinds. Among the missing transaction kinds and fact types, six transaction kinds are the same as the ones not included in the first case study. Since the importance of these six transaction kinds was already explained in Section 6.2, only the remaining four transaction kinds missing in the second case study will be explored.

The IT RM process of this case study does not include any transaction kind and fact type regarding the activity *Scope, Context and Criteria* of ISO 31000:2018. The purpose of this activity "is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment".

According to ISO 31000:2018, the RM process can be applied at different levels, so it is important to be clear about the scope under consideration, the objectives to be taken into account and their alignment with the organisational objectives. *T1 scope defining* of a process is fundamental in establishing the breadth of its IT RM activities. Additionally, it guides stakeholders to what must be considered in each assessment, and helps in justifying observations and other aspects of them. The process proposed by the case study starts with the identification of applicable threat scenarios based on the predefined threat scenarios instead of starting with scope definition [13].

This transaction kind is important since it dictates how the IT RM process will proceed. An organisation should define the scope and boundaries related to IT RM and identify all of the restrictions that affect the scope.

T2 context establishing is another transaction kind that is not part of the case study's process. Establishing the IT RM process context is crucial as it supplies the basis for establishing and justifying assertions within threat, asset, risk response effectiveness, and risk identification and assessment. Ideally, it also underpins the case for making treatment recommendations. The context is established taking into account the environment in which the organisation operates and "...should reflect the specific environment of the activity to which the risk management process is to be applied" [13].

The process of the case study considers the context of the online service (including the threats identified, their agents, and relevant assets) but, it does not establish the context of the IT RM process. However, the IT RM context establishment takes into account the context of the activity to which IT RM is to be implemented and in the case study, they consider the context of a particular online service. Therefore, the transaction kind T2 is partially present in the case study.

Another transaction that is not present in the case study is *T3 risk criteria defining*. ISO 31000:2018 defends that, the "organisation should specify the amount and type of risk that it may or may not take...define criteria to evaluate the significance of risk and to support decision-making processes". The stakeholders should ensure that criteria applied to assessments is consistent and aligns with the IT RM framework, and the criteria must be customised to the specific purpose and scope of the activity under consideration [13].

The risk criteria influences heavily the decisions made by the stakeholders and will be used during the whole process. Defining criteria must take into account the organisation's obligations, capacities and stakeholders' views [13]. This activity is important since it orientates stakeholders when making decisions and these decisions will be made considering the organisation's needs and limits.

According to PMBOK 6, *Plan Risk Responses* starts with the development of plans, by the nominated risk owner, for addressing every risk that is considered relevant, either because of the threat it poses to objectives or the opportunity it offers [65]. Contrarily, the IT RM process proposed by the case study starts with choosing the appropriate risk treatment option (risk modification, retention, avoidance, and sharing), that is equivalent to selecting strategies (*T12 risk responses strategies selecting*). This case study involves the activity *Plan Risk Responses* of PMBOK 6 except for one transaction kind of this activity, that is *T11 risk responses planning*. However, it includes the P-fact type resulting from this transaction kind that is *Risk Response*.

Table 6.2 shows the gaps (lack or excess of elements) identified in the case study and shows if the case study is completely lacking/exceeding those elements.

6.4 Case Study 3

In this case study, the risks' analysis is based on triad CIA (Confidentiality, Integrity, and Availability). It includes: (a) *Main impacts to the data holders if the risk occurs*; (b) *Main threats that can lead to risk*; (c) *Risk sources*; (d) *Controls to minimize risks*; (e) *Risks' severity, based on the potential impacts and implemented/planned controls*; and (f) *Risks' probability, regarding the threats, risks' sources,*

Table 6.2: Lack and excess of elements in case study 2

Excess	
Activities	*Level*
General threat scenarios identification	●
Specific threats identification	◐
Tasks prioritization	◐
Lack	
Transaction kinds	*Level*
T1 scope defining	●
T2 context establishing	◐
T3 risk criteria defining	●
T5 individual risks and sources of overall activity risk identifying	●
T9 quality of risks information evaluating	●
T10 risk owner identification	●
T11 risk responses planning	◐
T14 contingency plan developing	●
T15 risks enhancing	●
T16 risk responses implementation deciding	●

implemented/planned controls.

As can be noticed, most of the activities included in the analysis of risks are present in the essential IT RM process. However, the IT RM ontology does not contain two activities that are applied in the case study.

The essential model of IT RM does not contain any transaction kinds regarding the identification of threats, unlike this case study that identifies the *Main threats that can lead to risk*. The second case study also supports threats' identification, so the relevance of identifying threats to the essential model is explained in Section 6.3. The essential model partially includes this activity.

Risks' severity, based on the potential impacts and implemented/planned controls is also not included in the essential model of IT RM. In this case study, instead of assessing the priority of risks, the authors assess risks' severity. The severity of a risk is a 'String' and it depends on the potential impacts identified and the implemented/planned controls.

The priority of risks is somewhat equivalent to the severity of risks since a high priority risk is a very severe risk. However, the assessment of these two values is different since the priority of risks depends on the probability and impact of risks, while the severity of risks depends on the impact of risks and implemented/planned controls. Therefore, due to the similarities between both activities, the IT RM ontology partially includes the assessment of risks' severity.

The IT RM process of this case study does not include six transaction kinds, from which five are also missing in the first and second case study, namely *T5 individual risks and sources of overall activity risk identifying*, *T9 quality of risks information evaluating*, *T10 risks owner identification*, *T14 contingency plan developing*, and *T15 risks enhancing*. The relevance of these activities is explained in Section 6.2.

The transaction kind lacking in this case study that does not lack in the previous two case studies is *T6 risks priority assessment*. As mentioned above, instead of assessing the priority of risks, the authors assess the risks' severity. Both are similar and have the same purpose of evaluating risks, so the case study partially contains this transaction kind.

Table 6.3 shows the gaps (lack or excess of elements) identified in the case study and shows if the case study is completely lacking/exceeding those elements.

Table 6.3: Lack and excess of elements in case study 2

Excess	
Activities	*Level*
Main threats that can lead to risk	◐
Risks' severity, based on the potential impacts and implemented/planned controls	◐
Lack	
Transaction kinds	*Level*
T5 individual risks and sources of overall activity risk identifying	●
T6 risks priority assessment	◐
T9 quality of risks information evaluating	●
T10 risk owner identification	●
T14 contingency plan developing	●
T15 risks enhancing	●

6.5 Conclusion

The evaluation activity involved analysing the lack and excess of elements in each case study, comparing with the transaction kinds, P-fact types, and activities of the IT RM ontology. This analysis includes the purpose of the elements and their relevance to the essential model of IT RM.

The first case study proposes a novel IT RM framework due to the authors' dissatisfaction with current standards and frameworks [11]. The process of this case study contained one activity that was not part of the IT RM ontology and one that was part of the ontology but involved a task not included in the essential IT RM process. This case study lacks entirely five transaction kinds and partially one transaction kind.

The second case study proposes an IT RM framework based on a standard [52]. The process of this case study contained one activity that was not part of the essential model of IT RM and two activities that were implicit in the activities of the essential IT RM process. Regarding the lack of elements, this case study lacks entirely eight transaction kinds and partially two transaction kinds.

The third case study applies an IT RM process based on a popular standard. This case study contains two activities that are not completely included in the IT RM ontology and lacks entirely five transaction kinds and partially one transaction kind.

From the results obtained, it can be stated that the three case studies do not propose many activities not included in the essential IT RM process. However, the processes of the case studies lack some transaction kinds and corresponding P-fact types of the IT RM ontology.

The first two case studies do not involve expert judgment in their IT RM process, while the third case study partially involves expert judgment since it relies on specified entities to decide the implementation of planned mitigation strategies for risks. PMBOK 6 states that usually project managers rely on expert judgment to perform well. Expert judgment is one of the best-accepted approaches and is considered one of the best tools and techniques in RM processes.

Moreover, the case studies do not encompass check steps, such as evaluating the quality of risks' information, and preventive steps, such as developing a contingency plan. These steps are crucial to ensure the success of the IT RM process.

For future work, it is necessary to validate this proposal in more case studies to check if the lacking elements in both cases are essential or not. Additionally, to further analyse the compatibilities and gaps identified in the IT RM implemented by the "STAYAWAY COVID" in order to optimize the ontology of IT RM with the results obtained.

7

Conclusion

Contents

7.1 Conclusions

Currently, due to the advances in IT, organisations use and rely more on IT solutions to survive in the current market. Despite their benefits, IT solutions induct risks that may affect the achievement of the organisation's goals. To maximize the effectiveness of IT usage and to manage the risks associated with it, organisations implement IT RM [69].

If an organisation can manage risks successfully, it can modify them so that the organisation has more chances to meet its goals. Thus organisations must implement IT RM [16]. However, many organisations face difficulties in implementing this process successfully due to its diversity and complexity.

IT RM is diverse since numerous standards, frameworks, and related literature propose RM processes to deal with IT risks. These processes consist of different activities, causing a lack of consensus regarding the IT RM activities. Furthermore, IT RM is complex since it encompasses many concepts and relationships, and the conceptual intersection between them is weak.

The main objective of this research is to reduce the perceived complexity of IT RM, thus facilitating the understanding of this process, as well as to overcome this process's diversity by determining which are the most popular and essential activities of IT RM.

For this purpose, to overcome IT RM's complexity, it is proposed the definition of an ontology of IT RM to simplify and clarify this process and optimize its implementation using DEMO. Additionally, to overcome this process's diversity, it is proposed the execution of an SLR to review the essential and most popular IT RM activities implemented and recommended in the literature.

DEMO was chosen to produce an ontology of IT RM because [17]:

- DEMO supplies clear guidelines, therefore limiting the subjectivity in the modeling process;
- It has its roots on EO, and EO provides clear definitions for the constructs used in the DEMO models, hence reducing the degrees-of-freedom for the modeler, ensuring that the only one correct essential model is produced;
- DEMO models use a limited number of constructs (simplicity) and follow the transaction pattern (completeness and integrity), restricting the number of concepts that someone has to learn to understand the models.

Through DEMO models, one acquires an understanding of the organisation's essence that is comprehensive, coherent, consistent and concise [2].

The artifact is generic enough to be applied in any organisation that implements IT RM. Organisations can use the proposed IT RM ontology to identify any gaps of business transaction steps that occur during their IT RM process. The three demonstrations made in different case studies can confirm the previous statement.

Additionally, the ontology allows one to check if who is responsible for the transaction has the authority to do so, if the relationships and dependencies between the different transactions are present, among others. It was not possible to demonstrate these checks since the case studies did not provide enough information to do so.

To evaluate the solution proposed, the implication of each gap identified was studied to check if the missing transaction kinds are essential or not. The results obtained from the evaluation showed that both case studies do lack some transaction kinds contained in the essential model of IT RM and propose only one or two activities not included in the essential IT RM process defined.

The contributions of this work are: the identification and analysis of the key concepts (activities) and relationships of IT RM through an 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.

The principal contribution of this research work is the simplification and clarification of IT RM by facilitating its design, implementation, and assessment. Consequently, the chances of successfully implementing an essential IT RM process are increased.

7.2 Communication

During the execution of this research work, two peer-reviewed scientific papers were accepted in two different international conferences. The papers were:

- "On IT Risk Management Ontology using DEMO" (M. Rosa, S. Guerreiro and R. Pereira), accepted at the 12th International Conference on Knowledge Engineering and Ontology Development (KEOD 2020);

- "Designing an IT Risk Management Ontology Grounded on Systematic Literature Review" (M. Rosa, S. Guerreiro and R. Pereira), accepted at the Hawaii International Conference on System Sciences 2021 (HICSS-54).

Paper "On IT Risk Management Ontology using DEMO" briefly explains the SLR conducted and describes the proposal of this thesis, while "Designing an IT Risk Management Ontology Grounded on Systematic Literature Review" shows how it is possible to produce an ontology from the results of an SLR.

One article was submitted on journal Computers in Industry and is currently under review. This article is entitled "IT Risk Management process: a Systematic Literature Review" (S. Guerreiro, M. Rosa and R. Pereira). It describes extensively the SLR conducted and its results.

7.3 Limitations and Future Work

DEMO was used to develop an ontology of IT RM since it has many benefits, and allows the simplification and clarification of IT RM by reducing the process's complexity. However, it also has disadvantages. One of the disadvantages is the difficulty in understanding and implementing DEMO models, because of its specific notation. These models may be not easy to understand at first for those unfamiliar with the notation [17].

Moreover, DEMO models do not contain any implementation and realisation aspects. Even though this can be considered an advantage regarding flexibility and integration, it is not recommended to use DEMO as a standalone for communicating and reenacting IT RM process models to other parties. Hence the need to complement it with other techniques and models [17].

Initially, it was planned to demonstrate and evaluate this proposal through its implementation in a real organisation. The main goal of this demonstration and evaluation was to compare the key performance indicators of implementing the IT RM process with and without ontology. This way, it would be possible to verify if the ontology facilitates the implementation of IT RM and its improvement. However, due to COVID-19 and the consequent lockdown it was not possible to demonstrate and evaluate the solution this way. So, to demonstrate and evaluate the proposal, the ontology was applied on case studies to identify the gaps and compatibilities between the ontology and the case studies.

For future work, it would be beneficial to evaluate the completeness and validate the IT RM's essential model through its implementation in real-life case scenarios. With the results obtained, it could be verified if the IT RM's ontology meets or does not meet the desired objectives, by comparing its goals with the actual results from implementing the ontology. Furthermore, key performance indicators could be defined and assessed to measure the success of applying the ontology.

Bibliography

[1] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of management information systems*, vol. 24, no. 3, pp. 45–77, 2007.

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

[3] T. Oliveira and M. F. Martins, "Literature review of information technology adoption models at firm level," *Electronic Journal of Information Systems Evaluation*, vol. 14, no. 1, p. 110, 2011.

[4] S. D. Haes, W. V. Grembergen, and R. S. Debreceny, "Cobit 5 and enterprise governance of information technology: Building blocks and research opportunities," *Journal of Information Systems*, vol. 27, no. 1, pp. 307–324, 2013.

[5] K. Slyter. What is information technology? a beginner's guide to the world of it. [Online]. Available: https://www.rasmussen.edu/degrees/technology/blog/what-is-information-technology/

[6] H. L. Grob, G. Strauch, and C. Buddendick, "Applications for it-risk management–requirements and practical evaluation," in *2008 Third International Conference on Availability, Reliability and Security*. IEEE, 2008, pp. 758–764.

[7] S. L. Vrhovec and et al., "Diagnosing organizational risks in software projects: Stakeholder resistance," *International journal of project management*, vol. 33, no. 6, pp. 1262–1273, 2015.

[8] R. V. Bradley and R. M. Pratt, "Exploring the relationships among corporate entrepreneurship, it governance, and risk management," in *2011 44th Hawaii International Conference on System Sciences*. IEEE, 2011, pp. 1–10.

[9] J. Varajão and et al., "Iso 21500: 2012 and pmbok 5 processes in information systems project management," *Computer Standards & Interfaces*, vol. 50, pp. 216–222, 2017.

[10] E. Kutsch and M. Hall, "The rational choice of not applying project risk management in information technology projects," *Project Management Journal*, vol. 40, no. 3, pp. 72–81, 2009.

[11] S. Islam and et al., “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.

[12] S. Varga, G. Barreto, and P. D. Battaglin, “Increasing information systems availabiliy through accuracy, awareness, completeness and manageability of itsm,” in *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2019, pp. 1–4.

[13] ISO, “31000: 2018—risk management—guidelines,” vol. 262, 2018.

[14] T. Yaqoob and et al., “Framework for calculating return on security investment (rosi) for security-oriented organizations,” *Future Generation Computer Systems*, vol. 95, pp. 754–763, 2019.

[15] S. A. Torabi and et al., “An enhanced risk assessment framework for business continuity management systems,” *Safety science*, vol. 89, pp. 201–218, 2016.

[16] G. Purdy, “Iso 31000: 2009—setting a new standard for risk management,” *Risk Analysis: An International Journal*, vol. 30, no. 6, pp. 881–886, 2010.

[17] 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.

[18] J. L. Dietz and J. A. Hoogervorst, “Foundations of enterprise engineering,” 2017.

[19] A. P. Perinforma, “The essence of organisation,” *South Holland: Sapio Enterprise Engineering*, 2012.

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

[21] R. Mallett, J. Hagen-Zanker, R. Slater, and M. Duvendack, “The benefits and challenges of using systematic reviews in international development research,” *Journal of development effectiveness*, vol. 4, no. 3, pp. 445–455, 2012.

[22] B. Kitchenham and S. Charters, “Guidelines for performing systematic literature reviews in software engineering,” 2007.

[23] N. Rozzani, I. S. Mohamed, and S. N. S. Yusuf, “Risk management process: Profiling of islamic microfinance providers,” *Research in International Business and Finance*, vol. 41, pp. 20–27, 2017.

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

[25] A. Olechowski and et al., “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.

[26] 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.

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

[28] K. D. Bakker and et al., “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.

[29] S. Alhawari and et al., “Knowledge-based risk management framework for information technology project,” *International Journal of Information Management*, vol. 32, no. 1, pp. 50–65, 2012.

[30] J. Wang and et al., “A performance-oriented risk management framework for innovative r&d projects,” *Technovation*, vol. 30, no. 11-12, pp. 601–611, 2010.

[31] J. M. Yusta and et al., “Methodologies and applications for critical infrastructure protection: State-of-the-art,” *Energy policy*, vol. 39, no. 10, pp. 6100–6119, 2011.

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

[33] 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.

[34] 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.

[35] J. Webb and et al., “A situation awareness model for information security risk management,” *Computers & security*, vol. 44, pp. 1–15, 2014.

[36] 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.

[37] J. Oehmen and et al., “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.

[38] K. de Bakker and et al., “Risk managements’ communicative effects influencing it project success,” *International Journal of Project Management*, vol. 30, no. 4, pp. 444–457, 2012.

[39] 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.

[40] M. Ghaffari and et al., “Modeling and risk analysis of virtual project team through project life cycle with fuzzy approach,” *Computers & Industrial Engineering*, vol. 72, pp. 98–105, 2014.

[41] 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.

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

[43] M. E. Kara and et al., “A data mining-based framework for supply chain risk management,” *Computers & Industrial Engineering*, p. 105570, 2018.

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

[45] 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.

[46] H. P. Tserng and et al., “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.

[47] J. Mu and et al., “Effect of risk management strategy on npd performance,” *Technovation*, vol. 29, no. 3, pp. 170–180, 2009.

[48] D. Aloini and et al., “Modelling and assessing erp project risks: A petri net approach,” *European journal of operational research*, vol. 220, no. 2, pp. 484–495, 2012.

[49] 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.

[50] G. J. Correa-Henao and et al., “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.

[51] B. Barafort and et al., “Integrating risk management in it settings from iso standards and management systems perspectives,” *Computer Standards & Interfaces*, vol. 54, pp. 176–185, 2017.

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

[53] H. M. 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.

[54] F. Caron and et al., “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.

[55] S. Ni and et al., “A formal model and risk assessment method for security-critical real-time embedded systems,” *Computers & Security*, vol. 58, pp. 199–215, 2016.

[56] K. C. Demek and et al., “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.

[57] B. Barafort and et al., “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.

[58] Z. Ahmad and et al., “Building information modeling as a risk transformer: An evolutionary insight into the project uncertainty,” *Automation in Construction*, vol. 92, pp. 103–119, 2018.

[59] I. Kardes and et al., “Managing global megaprojects: Complexity and risk management,” *International Business Review*, vol. 22, no. 6, pp. 905–917, 2013.

[60] 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.

[61] 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*. IEEE, 2010, pp. 1207–1212.

[62] S. Schinagl and et al., “The revival of ancient information security models, insight in risks and selection of measures,” in *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2016, pp. 4041–4050.

[63] A. PMI, “guide to the project management body of knowledge (pmbok guide),” in *Project Management Institute (PMI)*, vol. 5, 2013.

[64] I. O. for Standardization, *ISO 31000: 2009: Risk Management: Principles and Guidelines*. International Organization for Standardization, 2009.

[65] A. PMI, “guide to the project management body of knowledge (pmbok guide), 6. ver,” *Project Management Institute(PMI)*, 2017.

[66] R. Pereira, R. Almeida, and M. M. da Silva, “How to generalize an information technology case study,” in *International Conference on Design Science Research in Information Systems*. Springer, 2013, pp. 150–164.

[67] R. K. Yin, *Case study research and applications: Design and methods*. Sage publications, 2017.

[68] B. S. ISO, “Iec 27005: 2011 british standard for information technology–security techniques–information security risk management,” *BSI standards Publication*, 2011.

[69] T. Ernawati and D. R. Nugroho, “It risk management framework based on iso 31000: 2009,” in *2012 International Conference on System Engineering and Technology (ICSET)*. IEEE, 2012, pp. 1–8.