IT RM Ontology from representation to optimization using Enterprise Ontology

Hugo Miguel da Silva Cruz

Thesis to obtain the Master of Science Degree in

Telecommunications and Informatics Engineering

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

Examination Committee

Chairperson: Prof. Ricardo Jorge Fernandes Chaves
Supervisor: Prof. Sérgio Luís Proença Duarte Guerreiro
Member of the Committee: Prof. Prof. Pedro Manuel Moreira Antunes de Sousa

November 2021
Acknowledgments

First and foremost, I have to thank my first supervisor, professor Sérgio Guerreiro. Without his assistance and dedicated involvement in every step throughout the process, who read my numerous revisions and helped establish some sense of the confusion.

In addition, I genuinely appreciate my second supervisor, professor Rúbén Pereira for his critical feedback and excellent guidance. Thanks a lot, you both.

Getting through my dissertation required more than academic support and I have many, many people to thank for listening to and, at times, having to tolerate me over the past six years. Some special words of gratitude and appreciation go to my friends who have inevitably been a key source of support when things would get a bit discouraging and seemingly unbearable.

I am enormously grateful for my parents and sister whose constant love and support kept me motivated. My accomplishments, success, and this dissertation stand as a testament to your unconditional love and belief. Deepest thanks to my grandparents, godparents, and uncles who keep me grounded, remind me of what is important in life, and are always supportive, without them I would not be who I am today.

Last but certainly not least, to my girlfriend, Maria Ferreira for constantly listening and put up with my days of complicated humor. The last 5 years have been a thrilling adventure, to find someone as special as you, out of all the people in the world, it sure is a daily blessing. I cherish the day that I encountered you, it remains the single most important encounter I have ever had. You’re my best friend and genuine love. Thank you for all the love, patience, and dedication. I am forever thankful for having you in my life.

My deepest appreciation to you all,
Hugo Cruz
Abstract

Information represents a valuable asset of an organization. With the technological advances in recent years, companies thoroughly rely on Information Technologies (IT) and their various advantages. However, IT bears various risks with it, in which Risk Management (RM) fulfills a critical support role. The ability to clearly identify IT risks, their impact, and their likelihood are important to allow for more efficient management of available resources. IT RM comprises measures that could be used to preserve IT assets, which can be easily related to maturity models responsible for defining levels at certain stages of maturity. When regarding IT RM maturity models, these various levels and their characteristics can be identified as a reference, establishing a process of evolution. We found considerations are necessary, not only about the management, prevention, combat, and monitoring of IT risks of a certain organization but also the development of a process and a culture that requires the availability of people and resources to be important to improve and support the IT RM process. In this thesis a maturity model will be proposed that will allow the assessment of maturity for any organization. This evaluation will be done using a data model composed of ontological elements extracted from the most popular activities in the available literature. A research methodology was used that will be based on the outcomes of the various iterations, producing artefacts that allow to solve the problems that arise and finally present the results obtained.

Keywords

IT RM; Ontology; Risk; RM; Maturity
Resumo

A informação representa um ativo valioso de uma organização. Com os avanços tecnológicos dos últimos anos, as empresas apostam fortemente nas Tecnologias de Informação (TI) e nas suas diversas vantagens. No entanto, as TI carregam consigo vários riscos, nos quais a Gestão de Risco (RM) desempenha um papel de suporte crítico. No entanto, as organizações têm dificuldades em implementar o RM de TI, uma vez que standards e frameworks incoerentes propõem diferentes processos para lidar com tais riscos. A capacidade de identificar claramente os riscos de TI, o seu impacto e a sua probabilidade são importantes para permitir um gestão mais eficiente dos recursos disponíveis. O RM de TI compreende medidas que podem ser usadas para preservar ativos de TI, que podem ser facilmente relacionados a modelos de maturidade responsáveis por definir níveis em determinados estágios de maturidade. No que diz respeito aos modelos de maturidade de RM de TI, os vários níveis e suas características podem ser identificados como uma referência, estabelecendo um processo de evolução. O modelo de maturidade proposto é baseado num processo de RM de TI de uma ontologia que tomou partido das atividades mais consensuais da literatura disponível e dos standards e frameworks sobre o assunto. Descobrimos que são necessárias considerações, não só sobre a gestão, prevenção, combate e monitorização dos riscos de TI de uma determinada organização.

Palavras Chave

IT RM; Ontologia; Risco; Modelo; Maturidade
# Contents

1 Introduction .................................................. 1
1.1 Problem definition ........................................... 3
1.2 Solution objectives ........................................... 3
1.3 Research Methodology ........................................ 4
1.4 Related Work .................................................. 5
1.5 Thesis Structure .............................................. 7

2 Background ................................................... 9
2.1 Design and Engineering Methodology for Organizations .............. 11
2.2 Systematic Literature Review .................................. 14
2.3 IT RM activities ............................................... 16

3 Applying IT RM into case studies ................................ 25
3.1 Development Process .......................................... 27
3.2 Argumentative validation using case studies ......................... 28
  3.2.1 Case Study 1 ............................................... 28
  3.2.2 Case Study 2 ............................................... 32
  3.2.3 Case Study 3 ............................................... 35
3.3 Conclusion .................................................... 38

4 Implementing IT RM ontology in an ER data model .................. 41
4.1 Development Process .......................................... 43
4.2 Data model validation ......................................... 45
  4.2.1 Case Study 1 ............................................... 45
  4.2.2 Case Study 2 ............................................... 45
  4.2.3 Case Study 3 ............................................... 47
4.3 Conclusion .................................................... 47

5 Developing a maturity model ...................................... 49
5.1 Development process ........................................... 51
5.2 Maturity model validation ...................................... 52
5.2.1 Case Study 1 ................................................................. 56
5.2.2 Case Study 2 ................................................................. 58
5.2.3 Case Study 3 ................................................................. 59
5.3 Conclusion ................................................................. 61

6 Conclusions ............................................................... 63
  6.1 Conclusions ............................................................... 65
  6.2 Limitations and Future Work ........................................... 66

Bibliography ............................................................... 67
List of Figures

1.1 DSRM used in this thesis ................................................. 5
2.1 DEMO aspect models adapted from [2] ............................... 13
2.2 Ontology development process [1] ...................................... 15
2.3 Systematic Literature Review phases ................................. 16
2.4 Organisation Construction Diagram developed in the IT RM ontology, using DEMO representation [1] ................................................. 23
2.5 Organisation Object Fact Diagram developed in the IT RM ontology, using DEMO representation [1] ................................................. 24
3.2 Completeness assessment for case study 1 ........................... 30
3.3 Completeness assessment for case study 2 ........................... 33
3.4 Completeness assessment for case study 3 ........................... 36
4.1 Data model obtained using the relations between transactions. ................................................. 44
5.1 Level 1 featured in the data model. .................................... 53
5.2 Level 2 featured in the data model. .................................... 54
5.3 Level 3 featured in the data model .................................... 54
5.4 Level 4 featured in the data model .................................... 55
5.5 Level 5 featured in the data model .................................... 56
5.6 Stayaway covid’s IT RM process maturity assessment ............ 57
5.7 GSRM’s IT RM process maturity assessment ......................... 59
5.8 OSSF’s IT RM process maturity assessment .......................... 60
List of Tables

2.1 Transaction kinds identified for each IT RM activity. ................................. 22
2.2 Transaction Product table adapted from [1] [3] .................................................. 23

3.1 Ontological comparison between the ontology’s IT RM process and the case study’s IT
    RM process  ........................................................................................................ 31
3.2 Ontological comparison between the GSMR process and the ontology’s IT RM process 34
3.3 Ontological comparison between the OSSF process and the ontology’s process ......... 37

4.1 Stayaway covid application implemented in the data model .............................. 46
4.2 GSRM implementation in the data model ......................................................... 46
4.3 OSSF implementation in the data model .......................................................... 48

5.1 Maturity model levels represented with their respective activities [4] ............... 52
5.2 Stayaway covid application assessed in the maturity model ............................... 57
5.3 GSRM assessed in the maturity model ............................................................. 58
5.4 GSRM assessed in the maturity model ............................................................. 60
Acronyms

ACM Association for Computing Machinery
AM Action Model
AIS Association for Information Systems
C-facts Coordination Facts
CIA Confidentiality, Integrity, Accessibility
CM Cooperation Model
DEMO Design and Engineering Methodology for Organisations
DS Design Science
DSRM Design Science Research Methodology
EO Enterprise Ontology
FM Fact Model
IADP Impact Assessment on Data Protection
IEEE Institute of Electrical and Electronics Engineers
IS Information Systems
ISO International Organization for Standardization
IT Information Technologies
IT RM Information Technologies Risk Management
OCD Organisation Construction Diagram
O-organisation Original Organisation
O-transactions O-organisation transaction kinds
P-acts Production Acts
P-facts Production Facts
PM Process Model
RM Risk Management
SLR Systematic Literature Review
SoI Scope Of Interest
SQL Structured Query Language
Tx Transaction Kind x
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Problem definition</td>
<td>3</td>
</tr>
<tr>
<td>1.2 Solution objectives</td>
<td>3</td>
</tr>
<tr>
<td>1.3 Research Methodology</td>
<td>4</td>
</tr>
<tr>
<td>1.4 Related Work</td>
<td>5</td>
</tr>
<tr>
<td>1.5 Thesis Structure</td>
<td>7</td>
</tr>
</tbody>
</table>
1.1 Problem definition

Currently, information represents a valuable and vital asset of an organization. With the technological advancements in recent years, companies have relied on Information Technology (IT) and its numerous advantages like availability, productivity, and cost-effectiveness but they also induce risks. Given the impact such risks have had on enterprises, organizations are craving innovative strategies, models, and more effective ways to manage risk. Enterprise ontology (EO) is an emergent knowledge field, applied to complex organizations when explicit definitions of competencies, responsibilities, authorities, and delegations are demanded. According to International Organization for Standardization (ISO) 31000 [5], risk is defined as "effect of uncertainty on objectives". To maximize the effectiveness of IT usage, organizations implement Risk Management (RM), more specifically in the IT RM specialization.

IT risks are defined as "an event or condition to have the possibility of causing a loss on the Information Systems (IS)" [6]. RM is a process composed of coordinated activities to direct and control an organization concerning risk [5]. If an organization has the ability to be successful at detecting and perceiving the risk, it can modify it to make it more likely to achieve the organization's goals. However, organizations have difficulties implementing such processes since several standards, frameworks, and related literature propose RM processes with various activities, which causes a lack of consensus. According to Becker "IT Management, therefore, needs supportive tools to assess the as-is situation of a company, derive and prioritize improvement measures and subsequently conduct the progress of their implementation." [7] Risk maturity models are believed to provide an accepted framework of benchmarks to assess the stage of risk management implementation." [8] These models are responsible for defining several levels at certain stages of maturity, this levels outline characteristics associated with different stages of maturity [9], they also set the necessary criteria for a continuous progression of the IT RM capability of a given organization. The maturity levels are organized from an initial level of more reduced capacity, in this case towards IT RM, to a sophisticated level corresponding to the state of the art in IT RM. According to Becker "While maturity models have been addressed in prescriptive, descriptive, and reflective works, the notions of maturity and maturity models have rarely been conceptualized in detail. [10], so given this, it seems appropriate to establish a maturity model for a subject in a state of rapid evolution and with little focus.

1.2 Solution objectives

As mentioned before, IT bears various risks with it, in which Risk Management (RM) fulfills a critical support role. Nevertheless, organizations struggle with implementing IT RM since incoherent standards and frameworks propose conflicting processes to deal with such risks. The ability to clearly identify IT risks, their impact, and their likelihood are important to allow for more efficient management of available
resources. IT RM comprises measures that could be used to preserve IT assets, which can be easily related to maturity models responsible for defining levels at certain stages of maturity. When regarding IT RM maturity models, these various levels and their characteristics can be identified as a reference, establishing a process of evolution. In this thesis, a maturity model will be proposed, grounded on an ontology's IT RM process taking advantage of the most consensual activities in the available literature and the standards and frameworks on this subject. The ontology will then be converted into a data model, in this way a more agile and direct comparison with the various processes analyzed will be possible. This analysis will obtain as an outcome the percentage of compliance with the maturity level of each activity proposed by the case studies. In this way, it will be possible to establish not only the level at which the organization is in terms of IT RM maturity, but it will also be possible to establish a path to follow, to increase maturity in this matter. We found considerations are necessary, not only about the management, prevention, combat, and monitoring of IT risks of a certain organization but also the development of a process and a culture that requires the availability of people and resources to be important to improve and support the IT RM process.

1.3 Research Methodology

Design Science (DS) represents a methodological path used in IT that is based on the outcomes of each iteration. It involves a process to design artifacts to solve observed problems, to then evaluate the designs, and finally to be able to communicate the results [11]. Peffers, Tuunanen, Rothenberger and Chatterjee [11] proposed a methodology development for DS because such a methodology might help IS researchers to produce and present high-quality design science research in IS that is accepted as valuable, rigorous, and publishable in IS research outlets. As follows, the proposed Design Science Research Methodology (DSRM) consists of 6 steps:

- Problem identification and motivation: Define the specific research problem and justify the value of a solution [11]
- Define the objectives for a solution: Infer the objectives of a solution from the problem definition and knowledge of what is possible and feasible [11]
- Design and development: Such artifacts are potentially constructs, models, methods, or instantiations [11]
- Evaluation: Observe and measure how well the artifact supports a solution to the problem [11]
- Communication: Communicate the problem and its importance, the artifact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences [11]
Resulting from the first iteration whose objective was to access the ontology’s, the first artifact was an IT RM application in case studies, in which the process proposed by the ontology will be compared with the processes proposed in chapter 2 section by the case studies presented in chapter 3.1. Thus, the objective will be to highlight the differences and also establishing the deficiencies found in each process. The second artifact will represent the development of a data model from case study 1 used in the previous iteration. In section 4 it is possible to examine the comparison of the various case studies with the proposed data model, hence undertaking the comparison and completeness assessment much more agile and optimized. The third and last artifact is the implementation of a maturity model. The case studies will be evaluated using the data model, this comparison will allow establishing the level of maturity that each organization is regarding the IT RM, and as important as understanding where an organization is to understand which path it will have to go to reach higher maturity levels.

In Figure 1.1, it can be seen the DSRM used and the different artifacts and stages in this thesis.

1.4 Related Work

Nowadays almost all organizational areas depend on IT support in their ordinary activities. Despite all its benefits like availability, productivity, and cost-effectiveness, it also induces risks in security and infrastructure reliability that must be managed according to standards and best practices [12], managing IT risks effectively is becoming a strategic and competitive business success factor, the objective is to reduce or control IT risks, by reducing its probability or if possible, mitigate its consequences. [13]. If an organization has the ability to be successful at detecting and perceiving the risk, it can modify it to make it more likely to achieve its goals [5].

IT risks are defined as “an event or condition to have the possibility of causing a loss on the Information Systems (IS)” [6].

RM is a process composed of coordinated activities to direct and control an organization concerning
risk [5]. To manage IT’s risk effectively, organizations implement a specialization of RM [14], which is IT RM, in this specialization RM activities are applied to manage IT risks. As mentioned before there are different IT RM processes proposed by other literature and standards.

An organization’s IT RM process according to Grob, Strauch and Buddendick must initially determine the goals in the context of the risk strategy (so the first activity would be Risk Strategy). Second, according to the goals established, identify and evaluate such risks (risk identification and risk analysis), thirdly, the IT risk analysis would serve as a basis to identify measures to mitigate the identified risks (risk governance), and lastly, the activity risk monitoring would serve to monitor how the mitigation measures affected the risks. [15].

Simultaneously, according to ISO 3100:2018, an organization’s process begins with the scope, criteria, and context definition, secondly a risk assessment is performed (like risk identification, analysis, and evaluation), this assessment serves as the basis for the following activity, Risk treatment, which identifies the mitigation measures to the identified risks. Finally, ISO 3100:2018 suggests a Monitor and review activity that would be identical to the “Risk Monitoring” activity proposed by Grob, Strauch, and Buddendick. Lastly, this standard proposes an activity “Recording and reporting,” that suggests, “the RM process and its outcomes should be documented and reported through appropriate mechanisms.” [5]

The framework proposed by Samejima and Yajima [6] begin with an information-gathering activity (“gather information about the information system and decide the goal of IT RM”). After establishing the goal, it is suggested the “IT risk assessment” activity (identify IT risks in the gathered information, estimate the loss and probability of each IT risk, based on this, it is established the treatment priority.). With the priority established, the next suggested activity is “risk treatment” as the name implies the mitigation measures are applied. After applying them, the activities “risk acceptance” and “risk observation”, which are “After reducing the IT risks, the managers judge whether the remained risks are acceptable or not.” and “observe results of IT Risk treatment” respectively. The final activity is “IT risk communication” which is “IS stakeholders share the information of the goal which is the evaluation of the IT RM” [6]

As can be seen from these examples, numerous standards, literature, and framework propose numerous processes, but sometimes possess many activities in common with different names. However, since the proposed processes have their limitation, new frameworks and standards are continuously being created [16]. Samejima and Yajima evaluate the framework’s effectiveness, by assuming two IT risk cases. In a case where the web service stops and a case where customer information is leaked, they concluded the framework can be adopted in a variety of IT risks after this evaluation. [6] Since all these examples propose various processes and ways of carrying out things, it is thought-provoking to consider the maturity of a particular company regarding its IT RM process. Maturity is defined as “an evolutionary progress in the demonstration of a specific skill or the achievement of an objective from an initial state to a desired final state” [17], in this case, the specific skill would be the ability to effectively manage the
various IT risks and how they optimize the value associated with their IT investments. Maturity models are responsible for defining several levels at certain stages of maturity, these levels outline characteristics associated with these different stages [9], they set the necessary criteria for a continuous progression of the IT RM capability of a given organization. According to Poeppelbuss and Roeglinger the maturity model application in practice, maturity models are expected to disclose current and desirable maturity levels and to include respective improvement measures. [18] The intention is to diagnose and eliminate deficient capabilities metaphorically refer to such tools as engines for continuously improving systems for guiding organizations and designing new entities. According to Poeppelbuss and Roeglinger, the following application-specific purposes of use are distinguished:

- "Descriptive: A maturity model serves a descriptive purpose of use if it is applied for as-is assessments where the current capabilities are assessed." [18]

- "Prescriptive: A maturity model serves a prescriptive purpose of use if it indicates how to identify desirable maturity levels and provides guidelines on improvement measures." [18]

- "Comparative: A maturity model serves a comparative purpose of use if it allows for internal or external benchmarking." [18]

The maturity levels are organized from an initial level of lower capacity towards IT RM to an advanced level corresponding to the state of the art in IT RM. [4] According to Fraser and Gregory [19] there are six basic components of maturity models, which are a certain number of levels, a descriptor for each level, a generic description or summary of the characteristics of each level, several activities for each dimension, a description of each activity as it might be performed at each level of maturity. The RM maturity model proposed by Proença, Borbinha, and Vieira [4] contains six maturity levels, one of which corresponds to level zero meaning that there is no RM process within the organization. The defined maturity levels are: Level 0 - Non-existent RM, level 1 - Initial RM, level 2 - Managed RM level 3 - Defined RM, level 4 - Quantitatively Managed RM and level 5 - Optimizing RM There is another maturity model proposed by Carcary [9] which possesses different names to the diverse levels (1 - Initial, 2 - Basic, 3 - Intermediate, 4 - Advanced and 5 - Optimising), however, they are remarkably similar regarding the classification of the various levels. As stated in the past, the levels of our maturity model are similar to other models that work and are thoroughly known, like the ones mentioned above. These models will be taken into account and adapted to the proposed model in terms of IT RM.

1.5 Thesis Structure

This thesis is arranged by the following sections.
• Chapter 2 identifies the background work. A theoretical study about the IT RM ontology background is elaborated, in this case grounded on the IT RM ontology proposed by [1, 3]. Starting with the study of the SLR performed by Rosa et al. [1] [3] for selecting the most popular and certified articles and arriving at the IT RM process with the most popular activities obtained in the SLR. Conclusively, it is standardized using DEMO (Design and Engineering Methodology for Organisations) to offer an ontology design. The most popular activities are described as well as the transaction kinds identified in each activity.

• Subsequently in chapter 3, the ontology is used to perform comparisons with other processes, establishing grammatical deficiencies and evaluating the completeness of the determining process in relation to the ontology. This way the ontology is implemented in a data model taking advantage of the relationships between the transactions evidenced in the ontology.

• The following chapter 4 the ontology is implemented in a data model taking advantage of the relationships between the transactions evidenced in the ontology.

• Next, in chapter 5, a maturity model is proposed, establishing levels to the IT RM process of a given company. Last but not least, in chapter 6

• Finally, in chapter 6 relevant conclusions are drawn and limitations and future work are established.
2 Background

Contents

2.1 Design and Engineering Methodology for Organizations ................. 11
2.2 Systematic Literature Review ................................................. 14
2.3 IT RM activities ................................................................. 16
2.1 Design and Engineering Methodology for Organizations

The SLR performed by [1] [3] provided the IT RM activities definitions, their relationships, dependencies, and who was responsible for what. Design and Engineering Methodology for Organizations (DEMO) was used to produce an Enterprise’s essential model, it was employed in this ontology because it offers significant simplifications and provides explicit concepts. In DEMO the organization’s essential model is composed of four aspect models [20]: the Cooperation model (CM), the Action model (AM), the Process model (PM), and the Fact model (FM). A Scope Of Interest (Sol) covers an organization, well defining what belongs to the Sol and what does not belong. To overcome IT RM’s complexity, it is stated that DEMO was used to simplify, clarify and also optimize the complexity of implementing an IT RM ontology. According to [1] [3] DEMO was chosen for the ontology implementation as it provides clear guidelines, therefore limiting the subjectivity in the modeling process, the definition of DEMO models uses greater simplicity, completeness, and integrity in its implementation since the number of constructs and follows a transition pattern. As said previously, DEMO is based on EO, it provides clear definitions of the possible constructs in DEMO models, this way it is possible to restrict the user to the sort of models he can create, making the model understandable to any DEMO user. According to Dietz, EO (Enterprise ontology) is the essential knowledge of the assembly and the operation of the organization of an enterprise, completely independent of the ways in which they are conceived and implemented. [21] EO supports an extensive scientific base and considerably reduces complexity, resulting in understanding To use EO in an organizational context, it is necessary to possess an extensive understanding of the essence of the organization that the model proposes. EO is nowadays a must-have in a company since it offers a coherent model from the point of view of the four aspect models forming a rational and integral, consistent whole, that is, the four models mentioned above do not present discrepancies between them and are concise, that is, there are no redundant matters in the conceptual model. This model will allow the assessment and resolution of problems and challenges that may arise. According to Dietz and Mulder, this conceptual model is an essential and ontological model, since it demonstrates the essence of the organization, independently of all aspects of implementation. According to PSI (Performance in Social Interaction), an actor is a human fulfilling an actor role, which means that this actor assumes the responsibility and must exercise this role. This responsibility conducts us to a necessary definition, which is the coordination act (C-act), these acts are made up of a performer, an addressee, an intention, and a product. As the name implies the performer and the addressee will both be human beings. At the end of the C-act, the outcome is the creation of a corresponding Coordination fact (C-fact). This C-fact will inevitably be the outcome of the C-act, so it is concluded that there will be a pattern of interactions between two roles (the performer and the addressee, which in this case can be considered initiator and executor), this interaction is called a transaction. According to Dietz and Mulder, there are three phases in a transaction, the order phase, the execution phase, and the result phase. The order phase will be
when the two actors, initiator, and performer, will agree on the product that will be brought in to satisfy the initiator’s request. The execution phase, as the name indicates, will be when the executing actor is producing the product and last but not least the result phase will be the negotiations between both actors about the delivered product. Every transaction corresponds to a unique transaction kind. This type of transaction produces an exclusive product and merely has a single actor role-playing the role of executor. To comprehend how the numerous actors are differentiated, it is necessary to perceive what a P-act (Production Act) is, which can be original, informational, and documentary. Original P-acts generate something original, new P-facts for example these acts include manufacturing, transporting, or devising a certain thing. Informational P-acts comprehend computing, remembering, and deriving facts. Documental facts involve data that hold facts and also files that hold data. This case would be for example saving, covering, and storing documents or data. Observing the types of P-facts described above, it is grasped that the original P-facts are the only ones capable of creating or altering an organization, thus, these types of p-facts will have to be made by an authorized and responsible actor, ie, the human beings in actor roles. In this manner, actor roles can be divided into three layers. These three distinctions are based on the types of P-acts as explained above:

- O-organization (Original-organisation)
- I-organization (Informational-organisation)
- D-organization (Documental-organization)

The essence of the organization is captured in the O-organization acts, thus, the fundamental elements of the core of an organization's model are the actor roles, C-acts, C-facts, P-acts and finally P-facts. The organization ontological model adapted from in DEMO Specification Language (DEMOSL)-3 consists of four integrated aspect models:

**Cooperation Model (CM)** of an organization's Sol is the ontological model of an organization, it identifies the transactor roles and the coordination structures among them, that is, identifies the actor roles (internal and external) and the transaction kinds. Actor roles within the focus organization are called internal. Transaction kinds of which both the initiator and the executor are internal actor roles are called internal transaction kinds. A CM is expressed in a Coordination Structure Diagram and a Transaction Product Table, possibly supplemented by a Bank Contents Table and a Bank Access Table.

**Action Model (AM)** of an organization's Sol is the ontological model of an organization's operation. For every internal actor role, it contains the rules that guide the role of fillers’ work. The guidelines for responding to coordination facts (C-facts) are called action rules; the guidelines for performing production acts (P-acts) are called work instructions. An AM is represented by Action Rule Specifications which guide the actor in performing coordinations acts perform and Work Instruction Specifications, which guides the actors in performing production acts.
Process Model (PM) of an organization’s Sol is the ontological model of the state space and the transition space of its coordination world. Regarding the state space, the PM contains, for all border transaction kinds, the process step kinds as well as the applicable existence. For the transition space, the PM contains, for all transaction kinds, the process step kinds as well as the applicable occurrence laws. A PM is expressed in a Process Structure Diagram.

At last, the Fact Model (FM) of an organization’s Sol is the ontological model of the state space and the transition space of its production world. Regarding the state space, the FM contains entity types, value types, property types, and attribute types that are relevant for the modeled organization as well as the existing laws that apply. Regarding the transition space, a FM contains the event types and the occurrence laws that apply. An FM is expressed in an Object Fact Diagram, supplemented by Derived Fact Specifications, and optionally supplemented by Existence Law Specifications.

In figure 4.1 it is shown how the four models relate with each other. The CM and AM cover both coordination and production while the PM regards only coordination and FM only production. As can be seen, the PM connects the CM and the AM regarding the coordination between actors. Oppositely, FM connects the CM and AM as far as production is concerned. By the figure, we can also conclude AM is the foundation on which the other three models are standing, meaning that they are already contained inside the AM, just need to be extracted.
2.2 Systematic Literature Review

In this section, an existing work by Rosa et al. [1] [3] based on a SLR aimed to synthesize IT RM activities in an ontology will be studied and evaluated its performance in concrete cases. RM is defined as "coordinated activities to direct and control an organization concerning risk" per ISO 3100 [5]. To manage IT risks effectively, organizations implement an RM specialization, which is IT RM, in this specialization RM activities are applied to manage IT risks. Although this process is regarded as important, organizations face difficulties implementing it, since known standards and frameworks and literature propose processes composed of different activities. To resolve such difficulties, Mariana Rosa performed a SLR based on the guidelines of Kitchenham (2004) to identify, evaluate and interpret all available and relevant data to research such topic, which in this case was gathering data concerning IT RM activities, either proposed or not proposed by standards and frameworks. This review only included articles written in English, and also only articles published in Journals or Scientific Magazines and Conferences were considered. This SLR was performed in four repositories, Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library, Association for Computing Machinery (ACM), Association for Information Systems (AIS), and ScienceDirect.

It is equally important to understand the filters used to restrict the results, given that the first set, which had no filters, resulted in a total of 4074 articles. The keywords used in all the repositories were "IT RM" AND "activities, OR "process" OR "stages" OR "frameworks". Regarding these keywords, five filters were used:

- The first filter searched for the chosen keywords on the article's title, or abstract, or article's author keyword. This retrieves all articles which have the defined keywords in their main topic.
- The second filter consisted of removing duplicate articles in the same repository and between repositories.
- The third filter consisted in removing articles that were not in English, articles that were not from journals/publications, and articles before 2009.
- The fourth filter involved the deletion of articles published in lower-ranked publications/journals.
- The fifth filter consisted in manually assessing article abstracts and introductions. Only articles covering the implementation of RM to IT risks, including articles, that implicitly or explicitly stated IT RM activities and articles that adopted an IT RM process proposed by known standards and frameworks were selected.

After the filtering process, the 50 articles that resulted from the filtration were subject to further analysis. After reading the 50 articles, some of them were withdrawn resulting in an ultimate set of
44 articles, which constituted the basis of this SLR’s findings. An extensive analysis was performed to establish the relationships and dependencies between the most popular IT RM activities and after it, it was determined a set of main and essential IT RM activities: Communication and Consultation, Context Establishment, Risk Identification, Risk Analysis, Risk Response Planning, Monitor and Control Risk, Recording and Reporting.

In figure 2.2 it is shown the process, from an SLR to an IT RM ontology.

Once the set was established, there was a need to find good and clear definition to all activities. For each article in the set, the data extracted were IT RM activities and if possible which standard or framework proposed those activities. Therefore the most popular activities are communication and consultation, context establishment, risk identification, risk analysis, risk response planning, monitor and control risk, recording, and reporting. In figure 3.2 it can be seen how the SLR process was performed.
2.3 IT RM activities

Before defining the essential model of IT RM, it was necessary to establish definitions of the most popular IT RM activities provided by the SLR. When referring to an organization, its essence is on its O-organisation (O stands from Original), where Original Production acts (P-acts) bring new, original, Production Facts (P-facts), these acts are performed by subjects in actor roles. The definition of the essential IT RM activities is necessary to identify the O-organisation transaction kinds (O-transactions), where P-acts are carried out by specific subjects in actor roles.

Communication and consultation

The purpose of this activity is to assist relevant stakeholders in understanding risk, the basis on which decisions are made, and the reasons why particular actions are required. According to ISO 3100:2018 communication seeks to promote awareness and understanding of risk and consultation involves obtaining feedback and information to support decision making [5]. Communication on risk and the way it is mitigated has an increasingly significant specificity: it must be efficient, particularly in times of turbulence. The second significant piece of this step of the RM process is consultation. There will be
someone whose job is to support those without technical experience in RM to acquire the expertise necessary for risk owners and others to accomplish their risk optimization goals and objectives.

**Context establishment**

According to the ontology used it is equivalent to scope, context, and criteria (according to ISO 3100:2018), these activities are responsible for defining the scope of RM activities, establishing the RM context from the organization’s external and internal environment, and defining the risk criteria. The organization should define the scope of its RM activities, that is, it is important to be clear about the relevant objectives to be considered and their alignment with organizational objectives.

When planning the approach, it should include the objectives and decisions that need to be made, the expected outcomes from the steps to be taken in the process, the time, location, specific inclusions and exclusion, appropriate risk assessment tools and techniques, required resources, responsibilities and records to be kept and the relationships with other projects, processes, and activities. Regarding the risk criteria, the organization should also specify the amount and type of risk that it may or may not be able to take, regarding the objectives. It should define criteria to evaluate the risk significance and to support decision-making processes. Regarding management systems information security, more specifically about the standard ISO 27001:2013, to establish the IT security management system (ISMS), it is necessary to align it with the organization’s strategic RM context in which the ISMS establishment and maintenance will occur.

[23] The context of the RM process should be established from the understanding of the external and internal environment in which the organization operates and should reflect the specific environment of the activity to which the RM process is to be applied. To determine external context, we should consider issues arising from its social, technological, environmental, ethical, political, legal, and economic environment, for example, economic shifts in the organization’s market or changes in technology. On the other hand, an organization’s internal context is the environment in which it aims to achieve its objectives. Internal context can include its approach to governance, its contractual relationships with customers, and its interested parties. Things that need to be considered are related to the culture, beliefs, values, or principles inside the organization, as well as the complexity of processes and organizational structure.

Three O-transactions were described in the ontology:

- **T1 scope defining**, the actor role is **A1 scope definer** it is both the initiator and the executor.

- **T2 context establishing**, the actor role is **A2 context establisher** it is both the initiator and the executor.

- **T3 risk criteria defining**, the actor role is **A3 risk criteria definer** it is both the initiator and the executor.
According to the ontology [1] [3] these transactions access the organisation's data.

**Risk Identification**

Risk identification is defined as "The purpose of risk identification is to find, recognize, and describe risks that might help or prevent an organization from achieving its objectives." Prior knowledge of the frequency, duration, and impact of the hazard is essential to effective RM and vulnerability reduction. The organization can employ a range of techniques for identifying uncertainties that may affect one or more objectives. There are several factors to be considered and also the relations between such factors should equally be considered such as the tangible and intangible risk sources, the causes and events, the threats and opportunities, and also the vulnerabilities. The organization should identify risks, whether or not their sources are under its control. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences. Two O-transactions were found:

- **T4 risks identifying**, the actor role is **A4 risk identifier** it is both the initiator and the executor.

- **T5 individual risks and sources of overall activity risk identifying**, the actor role is **A4 (initiator)** and **A5 subject matter proficient** is the executor.

As identified in the ontology [1] [3] 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 perform this activity, it is needed to access information resulting from T1, T2, T3 and also access data from the organisation.

**Risk Analysis**

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including the level of risk. In this section the analysis will regard qualitative analysis which evaluates the identified individual risk priorities utilizing the likelihood and the correspondent impact on the project’s objectives should the risk happen. [5]

**Qualitative Risk Analysis**

Qualitative risk analysis introduces a bias in the assessment of identified risks, therefore, it is necessary to be attentive to identify and correct them.

If a decision-maker is used to support the risk analysis activity, resolve partialities it is a significant part of the decision maker’s role. An assessment of the quality of available information on project risks also helps to clarify the assessment of the importance of each risk to the project. [5]

The qualitative risk analysis activity establishes the individual risk priorities regarding the risk response plan. It also identifies which risks should be treated and how, and it decides the most appropriate risk
treatment strategy and methods. An assessment of the quality of available information on risks in the project also helps to clarify the assessment of importance of each risk to the project, it also establishes the relative priorities of the individual risks of the project for the Plan Risk Responses process. Identifies a responsible person who will assume responsibility for planning an appropriate risk response and ensuring it is implemented.

Quantitative Risk Analysis

Quantitative risk analysis is the process of numerically analyzing the combined effect of identified risks and other uncertainty sources in the overall project objectives. The main benefit of this process is it quantifies the overall risk exposure of the project, and can also provide additional quantitative information from risks to support planning responses to them. [5] It utilizes information about individual risks previously evaluated in the qualitative risk analysis activity. To perform a robust analysis depends on the availability of high-quality data on individual project risks and other sources of uncertainty, as well as a solid underlying project baseline for scope, schedule, and cost. The risk’s quantitative analysis typically requires specialized software and expertise in the risk model's development and interpretation. Five O-transactions were found:

- **T6 risks priority assessment**, the actor role is **A6 risk analyser** it is both the initiator and the executor.

- **T7 risk probability of occurrence**, the actor role is **A6 (initiator) and A7 risks probability of occurrence assessor** is the executor.

- **T8 risks impact assessment**, the actor role is **A6 (initiator) and A8 risks impact assessor** is the executor.

- **T9 quality of risks information evaluating**, the actor role are **A7 and A8 (initiators) and A8 risks impact assessor** is the executor.

- **T10 risk owner identification**, the actor role is **A10 risk owners' identifier** it is both the initiator and the executor.

As identified in the ontology [1] [3] The transactions T7 and T9 are enclosed in T6, and T9 is enclosed in T7 and T8. In order to perform T6, T7 and T8, the executors need information from T4 and to perform the identify the risk owner activity, it is necessary to access data that resulted from performing T1, T2 and access organisation’s data.

Plan Risk Responses

Plan risk responses is the process of developing alternatives, selecting strategies, and agree on actions to deal with overall risk exposure, and also address individual project risks. Effective and appropriate
responses to risk can minimize individual threats, maximize opportunities, and reduce overall project risk exposure. This process also allocates resources and adds activities to project documents and the project management plan if it is necessary.

The main benefit of this process is that it identifies appropriate ways to address the overall risk and individual risks of the project. After risks have been identified, analyzed, and prioritized, plans must be developed by the person in charge indicated for the resolution of each individual risk that the project team considers to be a sufficiently important threat it poses to the project's objectives or the opportunity it offers.

The planned responses must be appropriate to the relevance of the risk, be cost-effective to meet the challenge, be realistic within the context of the project, agreed by all parties involved and have a designated person in charge. Secondary risks must also be identified. Secondary risks are risks that arise as a direct result of implementing a risk response. Often, a contingency reserves time or cost. Five O-transactions were found:

- **T11 risks responses planning**, the actor role is **A11 risk owner** it is both the initiator and the executor.
- **T12 risk responses strategies selecting**, the actor role is **A11 (initiator) and A12 strategies selector** is the executor.
- **T13 actions developing**, the actor role is **A11 (initiator) and A13 actions developer** is the executor.
- **T4 risks identifying**, the actor role are **A11 (initiator) and A4** is the executor.
- **T14 contingency plan developing**, the actor role is **A11 (initiator) and A14 contingency plan developer** is the executor.

As identified in the ontology [1] [3] 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.

**Implement Risk responses**

As the name implies, it is the process of implementing pre-agreed risk response plans. The benefit of this process is ensuring that agreed risk responses are carried out as planned in order to address overall project risk exposure, minimize individual threats, and maximize individual project opportunities.

A common problem with Project RM is that project teams commit efforts to identify and analyze risks and develop responses, and then responses are agreed upon and documented in the risk registry and report, but no action is taken to manage the risks. Two O-transactions were found:
- **T15 risks enhancing**, the actor role is **A15 risk responses implementer** it is both the initiator and the executor.

- **T16 risk responses implementation deciding**, the actor roles are A15 (initiator) and **A16 subject matter expert** is the executor.

As identified in the ontology [1] [3] *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.*

### Monitor risks

Monitor and Control risks serves the purpose of monitoring the implementation of risk response plans, also monitoring the evolution of identified risks as well as identifying and analyzing new risks and evaluating the RM process effectiveness. The main benefit of this process is that it enables project decisions based on current information on the overall risk exposure and individual project risks. To ensure that the project’s team and key stakeholders are aware of the current level of exposure to the risk, the project’s work must be constantly monitored for new, changed, outdated individual risks and for changes in the overall risk level of the project. The identified O-transactions for this activity are demonstrated in Table 3.1. Four O-transactions were found:

- **T17 implementation of risk responses monitoring**, the actor role is **A17 risk monitor** it is both the initiator and the executor.

- **T18 risk management process effectiveness evaluating**, the actor roles are A17 (initiator) and **A18 RM process effectiveness evaluator** is the executor.

- **T4 risks identifying**, the actor roles are A17 (initiator) and A4 is the executor.

- **T6 risks priority assessment**, the actor roles are A17 (initiator) and A6 is the executor.

As identified in the ontology [1] [3] *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

In this activity, the RM process and its results should be documented and reported through suitable mechanisms. Recording and reporting aims to communicate RM activities and outcomes across the organization, providing information for decision-making, improving RM activities, and at last assist interaction with stakeholders, including those with responsibility and accountability in RM activities.

It is also said that a regular review of the IADP referred to in this report is necessary, it is also said that
"An upcoming review is expected considering possible interoperability with similar systems from other states" According to ISO 3100:2018 "Reporting is an integral part of the organization’s governance and should enhance the quality of dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities. No O-transactions were identified for this activity.

Table 2.1: Transaction kinds identified for each IT RM activity.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Transaction kind</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context establishment</td>
<td>T1 scope defining</td>
</tr>
<tr>
<td></td>
<td>T2 context establishing</td>
</tr>
<tr>
<td></td>
<td>T3 risk criteria defining</td>
</tr>
<tr>
<td>Risk Identification</td>
<td>T4 risks identifying</td>
</tr>
<tr>
<td></td>
<td>T5 individual risks and sources of overall activity risk identifying,</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>T6 risks priority assessment</td>
</tr>
<tr>
<td></td>
<td>T7 risks probability of occurrence assessment</td>
</tr>
<tr>
<td></td>
<td>T8 risks impact assessment, the actor role</td>
</tr>
<tr>
<td></td>
<td>T9 quality of risks information evaluating</td>
</tr>
<tr>
<td></td>
<td>T10 risk owner identification</td>
</tr>
<tr>
<td>Plan Risk Responses</td>
<td>T11 risk responses planning</td>
</tr>
<tr>
<td></td>
<td>T4 risks identifying</td>
</tr>
<tr>
<td></td>
<td>T12 risk responses strategies selecting</td>
</tr>
<tr>
<td></td>
<td>T13 actions developing</td>
</tr>
<tr>
<td></td>
<td>T14 contingency plan developing</td>
</tr>
<tr>
<td>Implement Risk responses</td>
<td>T15 risks enhancing</td>
</tr>
<tr>
<td></td>
<td>T16 risk responses implementation deciding</td>
</tr>
<tr>
<td>Monitor risks</td>
<td>T17 implementation of risk responses monitoring</td>
</tr>
<tr>
<td></td>
<td>T18 risk management process effectiveness evaluating</td>
</tr>
<tr>
<td></td>
<td>T4 risks identifying</td>
</tr>
<tr>
<td></td>
<td>T6 risks priority assessment</td>
</tr>
</tbody>
</table>

As shown in Table 2.2, the TPT (Transaction Product Table) is a list of the transaction kinds and corresponding product kinds [1] [3].

In the ontology, the CM was the first model to be developed An Organisation Construction Diagram (OCD) was developed as demonstrated in figure 2.4. The actor roles are represented by squares and the O-transactions are presented by discs containing a red diamond. Solid black lines without a black diamond are called initiator links. This means that the actors in this role are allowed to initiate a transaction kind.

The solid black lines with a black diamond are called executor links. This means that the actors in this role are allowed to execute a transaction kind.

The black dashed lines are called information links. This means that actors in this role have access to the contents of the corresponding transaction bank. The transaction bank is defined as the *theoretical container of all facts that resulted from carrying out transaction kinds*. It is important to understand who are the initiator and executor actor roles in each O-transaction.
Table 2.2: Transaction Product table adapted from [1] [3]

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

Figure 2.4: Organisation Construction Diagram developed in the IT RM ontology, using DEMO representation [1]
As observed in figure 2.4 there are several activities in which the actor role is both the initiator and the executor.

The following model to analyze for the development of this thesis, is the FM, as mentioned earlier, this model connects the CM and AM of the organization, the OFD (Object Fact Diagram). The OFD adapted from [1] [3], where the “round angles” represent classes, for example, SCOPE, CONTEXT, and CRITERIA. The red diamonds represent the production even types that are the same as the product kinds shown in the 2.2 table. The diamonds displayed in the diagram are the product kind identifier, for example, P1, P2, among others. In figure 2.5, it can be seen the transaction and product kinds that were later used to establish the data model associated with the IT RM process proposed by the ontology.

Figure 2.5: Organisation Object Fact Diagram developed in the IT RM ontology, using DEMO representation [1]
3.1 Development Process

In this section, a direct comparison between the IT RM process proposed by the ontology described above and the IT RM process used in the Stayaway covid application will be presented, thus establishing the differences between both processes and also the deficiencies found in the establishment of the ontology's proposed process. To evaluate the ontology regarding its deficiencies [2] there’s a need to understand which deficiencies can be discovered.

An ontology construct in this context will be the IT RM process activities, proposed by the SLR performed, the grammatical construct will represent the IT RM activities regarding the STAYAWAY Covid.

In figure 3.1 we can see how to develop a transformation mapping [2], the article by Fettke and Loos gives an approach in the evaluation of reference models. The transformation mapping consists of two mathematical mappings, first, a representation mapping which describes how an ontology is mapped onto a grammar construct (for example, an organization's IT RM process), and secondly, an interpretation mapping, demonstrating how the grammatical constructs are mapped onto the ontology. There are four identified deficiencies of a grammar [2):

- **Incompleteness**: A grammar is incomplete if one of the ontological constructs is not corrected by one grammatical construct.

![Figure 3.1: Ontological deficiencies of a Grammar [2]](image)
• **Redundancy**: A grammar is redundant if an ontological construct (IT RM activity for example) cannot be mapped on exactly one grammatical construct, but can be mapped in more than one.

• **Excess**: A grammar is excessive if one of its constructs cannot be mapped onto an ontology construct.

• **Overload**: A grammar is overloaded if at least one of its constructs is mapped by more than one ontological construct.

A grammatical construct is "ontologically clear" if it is neither excessive nor overloaded so that it is defined unambiguously with respect to the interpretation. In tables 3.1 and 3.2.3 the "ontologically clear" is defined as "clear" in the "Grade" column of the table. [2] In these comparisons, it was decided that if there were transaction kinds of a given ontology activity present in the case study, this activity would be clear from an ontological point of view, that is, the activity of the IT RM process proposed by the ontology is present in the IT RM process of the case of study.

The objective of this artifact is to make sure the ontology has relevance within its universe since as stated before, there are several standards, frameworks, and literature on the topic even though there is no well-defined IT RM process with well-defined and ordered activities. In this way, the objective will be to test the ontology in real cases to validate it, to establish equivalences and differences between the various concepts used. Three case studies will be used in this assessment.

### 3.2 Argumentative validation using case studies

#### 3.2.1 Case Study 1

The STAYAWAY COVID app is a contact tracing system, using personal mobile devices, which has been developed in the context of the national health emergency resulting from the COVID-19 pandemic. In the document "Impact Assessment on Data Protection (IADP)" [24], the various application data protection’s risks are identified and analyzed, as well as the diverse activities that allow the management of such risks. In this case study, there is no definition of activities as in the others. There is, however, the exposure of the various activities that were taken in data protection, so the comparison will be more argumentative and interpretive of the IADP document.

In the IADP document [24], the scope and context of data processing is established, the purpose of its processing, the legitimacy of its purpose, the category of data that are the target of treatment, and someone is designated as treatment’s responsible. In this IADP activity, there were identified four transaction kinds and correspondent P-Fact types that are also present in the ontology those are: T1-scope defining, T2-context establishment and T3-risk criteria defining and also T10-risk owner identification.
In the following, there are two instances where the risks are identified, one of them using the CIA triad (Confidentiality, Integrity, Accessibility). There were identified two transaction kinds and their correspondent P-fact types that are also present in the ontology: T4-risks identifying and T5-Individual risk and source of overall activity risk identifying were performed two times.

After this, the CIA triad identified risks are analyzed establishing their likelihood and their impact. In the document it is also identified the main threats that can lead to the risks and main impacts that can happen if those risks do occur. In this activity four ontology transaction kinds and their correspondent P-Fact types were identified: T4 risks identifying, T7-risk probability of occurrence assessment, T8-risks impact assessment and T9-quality of risks information evaluating. In the subsequent activity, risk mitigation measures are identified. The document goes in-depth about three major risk mitigation strategies and also establish responses to the CIA triad. In this STAYAWAY covid activity we identified three transaction kinds and their correspondent P-Fact types: T11-risk response planning, T12-risk responses strategies selecting and T13-actions developing, these were performed two times. In the IADP document, it is stated that "the risks identified can be considered, in general, as satisfactorily mitigated, by counterbalancing them with organizational and technical measures proportionate to the impact and probability of occurrence of the identified risks"; so by this statement it can be concluded that the plans were implemented successfully.

In this activity there were identified two transaction kind and their respective P-Fact types:T15-risks enhancing and T16-risk responses implementation deciding. Finally, there are several instances where the monitoring activity is suggested. It is also stated that "the regular review of this impact assessment proves to be essential as a control and monitoring measure, safeguarding the need to implement additional measures to deal with risks detected in the meantime during the use phase, whether in the course of tests or already with wide adoption by the population". So, given this, we identified 4 transaction kinds and their respective P-Fact types: T17-implementation of risk responses monitoring, T18-risk management process effectiveness evaluating, T4-risks identifying and T6-risk priority assessment. The ontological deficiencies are identified in the table 3.1.

The assessment of the existence of mapping between the ontology IT RM process and the case study in question is shown in figure 3.2.
In table 3.1, it can be seen the evaluation between the Ontology’s IT RM process and the activities carried out in the STAYAWAY Covid’s system.
### Table 3.1: Ontological comparison between the ontology’s IT RM process and the case study’s IT RM process

<table>
<thead>
<tr>
<th>Ontology</th>
<th>Stayaway covid app</th>
<th>Grade</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Consultation</td>
<td>Articles and news about the system.</td>
<td>Clear</td>
<td>There are several articles about this app either given by the government or other institute</td>
</tr>
<tr>
<td>Context establishment</td>
<td>Scope and context defining, processing purpose, its legitimacy and treated data categories</td>
<td>Clear</td>
<td>In the IADP document it is described how data is treated and is very similar to the activity proposed in the ontology.</td>
</tr>
<tr>
<td>Risk Identification</td>
<td>Risk identification and CIA triad analysis</td>
<td>Redundancy</td>
<td>There’s redundancy since 1 ontological construct matches with 2 grammar constructs</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>Quantitative and qualitative analysis by the CIA triad.</td>
<td>Clear</td>
<td>This grammatical construct is ontologically clear, because there is a match between the activity done and the proposed one.</td>
</tr>
<tr>
<td>Plan Risk responses</td>
<td>There are two instances where there are identified risk measures</td>
<td>Redundancy</td>
<td>There is redundancy since there are 2 sets of plans, one for each risk identification activity.</td>
</tr>
<tr>
<td>Implement Risk Response</td>
<td>In the document there is a statement, saying the risks were satisfactorily mitigated</td>
<td>Clear</td>
<td>This grammatical construct is ontologically clear, because there is a match between the activity done and the proposed one.</td>
</tr>
<tr>
<td>Recording and Reporting</td>
<td>The IADP document itself is a type of recording and reporting activity</td>
<td>Clear</td>
<td>This grammatical construct is ontologically correct, because there is a match between the activity done and the proposed one.</td>
</tr>
</tbody>
</table>

In table 3.1 it can be perceived that most of the ontology’s activities were covered in the IT RM process of the stayaway covid application, it was also identified two instances where there is a redundancy deficiency. In one of these instances, there are two activities to identify risks, *risk identification* and *plan risk identification*, this double identification also leads to double planning of responses that constitute the redundancy deficiency. As stated by Fettke [2] a grammatical construct is adequate if it is defined unambiguously with respect to the interpretation mapping, given this, a redundancy grade was assigned. This comparison constitutes the first artifact obtained with the research methodology shown in figure 1.1.
3.2.2 Case Study 2

In the second case study, retrieved from the "An empirical study on the implementation and evaluation of a goal-driven software development risk management model" [25] we have a case that aims to develop a software product to satisfy market demand as quickly as possible, therefore allowing a competitive advantage to the company, the case proposes a "Goal-driven Software Development Risk Management Model (GSRM)". It is, however, identified that there are many uncertainties and risks at all stages of development, these will have a considerable influence on the uncertainty and success of the product in question. It is identified that the objective would be to introduce guidelines that would explain where missing RM activities would be inserted. This case study uses Goal-driven Software Development Risk Management Model. This framework consists of 4 layers to support RM software development RM:

Goal layer: This layer focuses on the factors that contribute to the success and completion of the project and the activities that comprise it. These objectives are specific to each project and have to do with economic characteristics, quality, user satisfaction, among others.

Obstacle layer: It is stated that "obstacles represent the prime causes that reduce the ability to achieve a certain or certain goals" That is, this layer must be aligned and all obstacles must derive from each category of objectives.

Assessment layer: In this layer, events are quantified as a consequence of multiple risk factors. It is stated that "this layer precisely annotates individual risk events and it establishes the causal relationship model between risk factors and related risk events. It also focuses on the severity of the risk events’ impact to goals”

Treatment Layer: This layer focuses the measures necessary to counter risks to fulfill the identified business goals. It is also stated that in this layer it is measured the effectiveness of the actions taken as well as the identification of new risks that can appear during the development.

The GSRMR proposes several activities that "are required for goal-driven risk management" [25], the first activity is to initialise goal-driven RM during the requirements engineering phase, it is said that this activity defines the RM scope and follows ISO 3100:2009 [5] identifying the RM context as well. In this activity three transaction kinds were identified $T1$-scope defining, $T2$-context establishing and $T3$-risk criteria defining. [1] [3] The next activity is "Identify and model goals" whose function is to develop and map components according to the project success indicators, meaning that the objective is to identify and categorize goals to provide context and meaning to their project contributions. No transaction kinds were identified in this activity.

The following activity is "identification and modelling of obstacles", in this activity risk factors are identified, which are considered the primary cause of obstacles and are also considered responsible for risk events. In this activity one transaction kind was identified $T4$-risks identifying. [1] [3] The next activity is "Assess risks, as the name implies is the risk assessment by estimating its impact, priority and
In this activity three transaction kinds were identified **T6-risks priority assessment**, **T7-risks probability of occurrence assessment** and **T8-risks impact assessment**. [1] [3] This activity assesses risk by estimating the risk level and relevant priority. We start with the causal relationship model by following risk factors and associated risk events as a consequence. This allows us to focus on the relevant risk events for the risk level estimation, rather than considering all raw risk factors. Risk estimation considers risk event likelihood and its severity of impact on goal negation. The impact assessment builds the cause-consequence relationship from the risk event to the obstructed goals. The risk assessment finally prioritizes the risk so that high prioritized ones get immediate attention. The risks are given different scales of priority, this allows the highest levels of attention to be directed towards the highest priority risks.

The next and last activity "Treat and monitor risks" intends to manage the risks and monitor the effectiveness of this control. It is, in addition, stated that “Risk treatment needs to be planned and mapped with the risk management scope.” [25] Once the control actions are implemented, this activity will monitor the same risks throughout the project. In this activity five transaction kinds were identified **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**. [1] [3]

The assessment of the existence of mapping between the ontology IT RM process and the case study in question is shown in figure 3.3, this assessment was carried out using the information in the documentation regarding the case study. [25]

![Figure 3.3: Completeness assessment for case study 2](image)

In table 3.2.3, it can be seen the evaluation between the Ontology's IT RM process and the activities
carried out in the Goal-driven Software Development Risk Management Model. In this table it can be perceived that most of the ontology’s activities were covered in the IT RM process of the stayaway covid application, it was also identified three instances where there is an overload deficiency, since if at least one of GSRM’s activities is mapped by more than one ontological activity. Despite the existence of at least one of the transaction kinds of each activity of the IT RM process proposed by the ontology, transaction kinds were identified that are not covered by the case study. In this case, the transaction kinds 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 implementing decision were not covered. [1] [3] This comparison constitutes the first artifact obtained with the research methodology shown in figure 1.1

<table>
<thead>
<tr>
<th>Table 3.2: Ontological comparison between the GSMR process and the ontology’s IT RM process</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ontology</strong></td>
</tr>
<tr>
<td>Communication Consultation</td>
</tr>
<tr>
<td>Context establishment</td>
</tr>
<tr>
<td>Risk Identification</td>
</tr>
<tr>
<td>Risk Analysis</td>
</tr>
<tr>
<td>Plan Risk responses</td>
</tr>
<tr>
<td>Implement Risk Response</td>
</tr>
<tr>
<td>Recording and Reporting</td>
</tr>
</tbody>
</table>

This process has five activities and during the analysis of these, twelve transaction kinds [1] were identified, their respective P-fact types, 3 overload deficiencies, and one incompleteness deficiency [2].
In other words, for the first time, we arrived at an activity that was not mappable in the case study. The overload deficiency is due to the fact that three activities of the process proposed by the ontology (Plan Risk Responses, Implement Risk Response, and Recording and Reporting) are mapped by the Treat and Monitor Risks activity of the GSRM process.

3.2.3 Case Study 3

In the third case study, adapted from the article “Introducing OSSF: A framework for online service cybersecurity risk management” a new framework for online security RM services is proposed with the particularity that can be used by service providers and consumers. This framework is called Online Services Security Framework (OSSF). The framework is based on the Threat model, the Risk model, and the Meta-model, it is stated that “Both Threat model and Risk model are considered an important autonomous part of the Meta model which describes the whole framework.” The threat model is in charge of facilitating awareness and identification of all possible threat scenarios that may occur in an online service context. This template is stated that it is “focused on provider's and consumer’s viewpoints”, this means that threats that may occur from the surrounding environment are unconsidered. The Risk model is in charge of identifying, assessing in qualitative terms the severity of risks and also their treatment. In this model, the RM process is proposed in accordance with the ISO/IEC 27005:2011 standard and it is said that the process design is suitable for recurrent and frequent iterations. It’s composed by:

The first activity is General threat scenarios identification based on the threat model, which can arise in a specific context of an online service This activity does not correspond to any activity in the ontology.

The next activity is Specific threats identification which, based on a list of the previous activity, selects suitable threat categories and is also considered the current context in order to be considered a "more detailed description of threats including threat agents and relevant assets." [26] In these activities, no similarities were recognized with the process proposed by the ontology. The following activity is Risks identification and assessment, which involves the identification and description that comes from threats, their assessment, and how these risks affected the assets’ vulnerabilities. Four transaction kinds were identified in this activity T4-risks identifying, T6-risks priority assessment, T7-risks probability of occurrence assessment, T8-risks impact assessment. [1] [3]

The subsequent activity is the risk treatment in which, as the name implies, decisions on the treatment options for the various risks are made. One transaction kind was identified in this activity T12-risk responses strategies selecting. [1] [3]

Identification of suitable tasks is the following activity. This activity focuses on the identification of tasks to implement the risk treatments agreed upon in the previous activity. This activity bears no similarities with any of the process proposed by the ontology. In this activity the T13-actions developing transaction kind was identified. [1] [3]
The next activity is the tasks prioritization, here the priority of the tasks ordering them based on the associated risk and score is established. The score is given by the sum of the risk likelihood and impact. This activity was unidentified in the ontology. Tasks execution focuses on the performance of the execution of pre-agreed on activities, it also monitors their status. One transaction kind was identified in this activity T17-implementation of risk responses monitoring. [1] [3]

The last activity in the process is Review of results and benefits of finished tasks, this activity aims to determine whether the tasks performed contributed to the reduction of risk. In this activity, one transaction kind was identified T18-risk management process effectiveness evaluating. [1] [3]

The assessment of the existence of mapping between the ontology IT RM process and the case study in question is shown in figure 3.4, this assessment was carried out using the information in the documentation regarding the case study. [26] 

![Figure 3.4: Completeness assessment for case study 3](image)

In Table 3.3, it can be seen the evaluation between the Ontology’s IT RM process and the activities carried out in the OSSF IT RM process. In this table it can be perceived that most of the ontology’s activities were covered in the IT RM process, it was also identified three instances where there is an excess deficiency, given that there is no correspondence of any ontological process activity. It was also identified a case of redundancy deficiency, since there are more than one case study activities mapped by one ontological activity.

As in Table 3.3 there were also identified two cases where there is an overload deficiency, since one case study activity is mapped by more than one ontological activity. Despite the existence of at least one of the transaction kinds of each activity of the IT RM process proposed by the ontology, transaction kinds were
identified that are not covered by the case study. In this case, the transaction kinds identified are T5-individual risks and sources of overall activity risk identifying, T1-scope defining, T2-context establishing, T3-risk criteria defining, T9-quality of risks information evaluating, T10-risk owner identification, T11-risk responses planning, T14-contingency plan developing, T15-risks enhancing, and T16-risk responses implementing decision were not covered. [1] [3]

This comparison constitutes the first artifact obtained with the research methodology shown in figure 1.1.

In table 3.3, it can be seen the evaluation between the Ontology's IT RM process and the activities carried out in GSRM system [26].

<table>
<thead>
<tr>
<th>Ontology Activity</th>
<th>OSSF Activity</th>
<th>Grade</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Consultation</td>
<td></td>
<td>Incompleteness</td>
<td>This activity is not covered in the case study</td>
</tr>
<tr>
<td>General threat scenarios</td>
<td></td>
<td>Excess</td>
<td>This activity is not covered in the ontology</td>
</tr>
<tr>
<td>Specific threats identification</td>
<td></td>
<td>Excess</td>
<td>This activity is not covered in the ontology</td>
</tr>
<tr>
<td>Context establishment</td>
<td></td>
<td>Incompleteness</td>
<td>This activity is not covered in the case study</td>
</tr>
<tr>
<td>Risk Identification</td>
<td>Risk Identification and treatment</td>
<td>Overload</td>
<td>There is an overload since it exists 1 case study activity for several ontological activities</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>Risk Identification and treatment</td>
<td>Overload</td>
<td>There is an overload since it exists 1 case study activity for several ontological activities</td>
</tr>
<tr>
<td>Plan Risk responses</td>
<td>Risk treatment and Identification of suitable tasks</td>
<td>Redundancy</td>
<td>There's redundancy since 1 ontological construct matches with 2 grammar constructs</td>
</tr>
<tr>
<td>Tasks prioritization</td>
<td></td>
<td>Excess</td>
<td>This activity is not covered in the ontology</td>
</tr>
<tr>
<td>Implement Risk Response</td>
<td>Tasks execution</td>
<td>Clear</td>
<td>This grammatical construct is ontologically clear, because there is a match between the case study activity done and the ontology's activity.</td>
</tr>
<tr>
<td>Recording and Reporting</td>
<td>Review of results and benefits</td>
<td>Clear</td>
<td>This grammatical construct is ontologically clear, because there is a match between the case study activity done and the ontology's activity.</td>
</tr>
</tbody>
</table>

In the third and last case study, OSSF [26] proposes another IT RM process containing eight activi-
ties. During the analysis of this process, eight transaction kinds, their respective P-Fact types, and eight grammar deficiencies were identified. There are two deficiencies of incompleteness, three deficiencies of excess, two deficiencies of overload, and one of redundancy. As stated earlier, incompleteness deficiencies are examples of activities that are not mapped by ontology. These activities are Communication and Consultation and Context Establishment. The Excess deficiency is the first time ontology is unable to map an activity proposed by the case study, which could jeopardize the completeness of the ontological IT RM process. These activities, that were not mappeable, were General Threat Scenarios, Specific Threats identification, and Task prioritization. The overload activities will be Risk Identification and Risk Analysis, which are fulfilled by the Risk Identification and Treatment activity proposed by the case study, meaning there is one activity that contains all the actions proposed in those activities.

Finally, the identification of a redundancy deficiency means there are two activities proposed by the case study, risk treatment and identification of suitable tasks, that are covered by only one ontology activity, which is the plan risk responses activity.

3.3 Conclusion

In the first assessment, the completeness of the IT RM process proposed by the ontology was tested using three case studies. This analysis constituted the second assessment using the IT RM process and its transaction kinds, as well as the first artifact demonstrated in the DSRM1.1.

- In the first case study, the stayaway covid application, in particular the IADP [24], does not propose a new IT RM process but takes advantage of some framework methodologies proposed by the ISO 31000:2009 standard [5]. The objective of the analysis carried out was to identify the grammatical deficiencies in the process presented by the ontology. In this case study, twelve transaction kinds were identified [1], their corresponding P-facts types, and two redundancy deficiencies, that is, there are two activities proposed by the ontology that are executed more than once in the stayaway covid application, these activities are Risk Identification and Plan Risk Responses. [2]

- In the second case study, GSRM [25] proposes a new framework with clear guidelines on how to implement IT RM. This process has five activities and during the analysis of these, twelve transaction kinds [1] were identified, their respective P-fact types, 3 overload deficiencies, and one incompleteness deficiency [2]. In other words, for the first time, we arrived at an activity that was not mappable in the case study. The overload deficiency is due to the fact that three activities of the process proposed by the ontology (Plan Risk Responses, Implement Risk Response, and Recording and Reporting) are mapped by the Treat and Monitor Risks activity of the GSRM process.
In the third and last case study, OSSF [26] proposes another IT RM process, this process follows the ISO 27005:2011 [27] standard and contains eight activities. During the analysis of this process, eight transaction kinds, their respective P-Fact types, and eight grammar deficiencies were identified. There are two deficiencies of incompleteness, three deficiencies of excess, two deficiencies of overload, and one of redundancy. As stated earlier, incompleteness deficiencies are examples of activities that are not mapped by ontology. These activities are Communication and Consultation and Context Establishment. The Excess deficiency is the first time ontology is unable to map an activity proposed by the case study, which could jeopardize the completeness of the ontological IT RM process. These activities, that were not mappable, were General Threat Scenarios, Specific Threats identification, and Task prioritization. The overload activities will be Risk Identification and Risk Analysis, which are fulfilled by the Risk Identification and Treatment activity proposed by the case study. Finally, the identification of a redundancy deficiency means there are two activities proposed by the case study that is covered by only one ontology activity.
Implementing IT RM ontology in an ER data model

Contents

4.1 Development Process ........................................... 43
4.2 Data model validation ........................................... 45
4.3 Conclusion ......................................................... 47
4.1 Development Process

In this section, the transition from ontology to a data model from the transactions identified in Table I will be discussed. The identification of transactions enclosed in others will allow establishing the relationships between the various tables created to allocate the data. This identification was performed by Rosa in the transaction description [1], the different transactions are displayed in Table I. Given this, a Structured Query Language (SQL) data model was established in which the necessary tables would be identified to simulate all the transitions and therefore the activities that make up the IT RM process. The transactions that make up the "Context Establishment" activity T1- Scope defining, T2-Context Establishment and T3-Risk Criteria Defining access the organization's data. Three tables were defined: the Scope table, the Context table and the Criteria table. In Figure 3, it can be perceived the tables, their variables and the relationships between each other.

Regarding the transactions that make up the "Risk Identification" activity T4-risks identifying, T5-individual risks and sources of overall activity risk identifying, as identified in the ontology [1] "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 perform this activity, it is required to access information resulting from T1, T2, T3 and also access data from the organisation. To carry out these two transactions, it would be necessary to have a risk table with its various characteristics such as its owner and the priority assigned to it, in addition given the necessity for T5 it will also be stored the source for each risk, since this will be important in the analysis and response planning activity. In Figure 3 it can be seen both tables, their variables and since as said before T5 is enclosed in T4, there is a relationship between both tables regarding the identified risks. Regarding the transactions that make up the "Risk Analysis" activity T6-risks priority assessment, T7-risks probability of occurrence assessment, T8-risks impact assessment, T9-quality of risk’s information evaluating, T10-risk owner identification, As identified in the ontology [1] The transactions T7 and T9 are enclosed in T6, and T9 is enclosed in T7 and T8. To perform this activity, the executors require information from T4 and to perform the identify the risk owner activity, it is required to access information resulting from T1, T2 and also access data from the organisation.

As previously mentioned, to be able to carry out the analysis transactions in the data model, it will be necessary to manipulate the variables in the Risk and Individual Source table, like the identification of the risk itself, the identification of its source and its priority. However, as previously stated, the priority is imposed by the impact of the risk, by its probability and these depend on the quality of the risk's information, so it was necessary to introduce a new table, the Priority table, as the name indicates identifies the risk's impact, probability and the quality. As stated before the activity’s executors need to access information from T4-risks identifying, so there is a relation set on the risk variable between the Priority and the Risk tables as can be seen in Figure 3. The transactions that make up the "Plan Risk Responses"
activity **T11-risks responses planning**, **T12-risk responses strategies selecting**, **T13-actions developing**, **T4-risks identifying**, **T14-contingency plan developing** as identified in the ontology [1] 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.

The risk response, the strategy used, the actions to be taken and the contingency plan will depend on the priority level of each risk as stated in the ontology. It is this priority that is the relation between the priority and response plan tables. Regarding the transactions that make up the “Implement Risk responses” activity **T15-risks enhancing**, **T16-risk responses implementation deciding** as identified in the ontology [1] 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. To implement the plans, it is necessary to identify the established strategy, the actions to be taken and the contingency plan, hence there is a relationship between the response plan table and the response implementation table that crosses these variables with another one that symbolizes the fulfillment of these plans. Regarding the transactions that make up the “Monitor risks” activity **T17-implementation of risk responses monitoring** and **T18-risk management process effectiveness evaluating**, as identified in the ontology [1] The transactions T4, T6 and T18 are enclosed in T17. To monitor the implementation of risk responses, it is necessary to access T15. Meaning that these transactions will have to access the risk, response and priority implementation tables.

![Data model obtained using the relations between transactions.](image)

**Figure 4.1:** Data model obtained using the relations between transactions.
The dotted lines establish the relations in terms of foreign keys between the tables as described in the ontology. A foreign key is a column of a certain table in a relational database whose values match other values in another table in that same database. This data model implementation will allow a more agile comparison with any given IT RM process.

4.2 Data model validation

4.2.1 Case Study 1

As stated before the STAYAWAY COVID app is a contact tracing system, using personal mobile devices, which has been developed in the context of the national health emergency resulting from the COVID-19 pandemic. The scope and context of data processing is established, the purpose of its processing, the legitimacy of its purpose, the category of data that are the target of treatment, and someone is designated as treatment's responsible. Consecutively there are two instances where the risks are identified, one of them using the Confidentiality, Integrity, Accessibility (CIA) triad. The CIA triad is therefore identified risks are analyzed establishing their likelihood and their impact. Risk mitigation measures are consequently identified. The document goes in-depth about three major risk mitigation strategies and also establish responses to the CIA triad. "The risks identified can be considered, in general, as satisfactorily mitigated, by counterbalancing them with organizational and technical measures proportionate to the impact and probability of occurrence of the identified risks". "The regular review of this impact assessment proves to be essential as a control and monitoring measure, safeguarding the need to implement other measures to deal with risks detected in the meantime during the use phase, whether in the course of tests or already with general adoption by the population". Once the activities have been identified, we proceeded to the maturity assessment based on the proposed model.

As can be seen in table 4.1 it is possible to verify that all activities can be modeled using the existing arguments in the data model. The arguments that were validated in the model were identified in the IADP documentation.

4.2.2 Case Study 2

As used in section 2 of chapter 3.1. The second case study, retrieved from the "An empirical study on the implementation and evaluation of a goal-driven software development risk management model" [25] we have a case that aims to develop a software product to satisfy market demand as quickly as possible, therefore allowing a competitive advantage to the company, the case proposes a "Goal-driven Software Development Risk Management Model (GSRM)". It is, however, identified that there are many uncertainties and risks at all stages of development, these will have a considerable influence on the uncertainty
Table 4.1: Stayaway covid application implemented in the data model

<table>
<thead>
<tr>
<th>Impact Assessment on Data Protection (Stayaway Covid app)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Study 1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Scope and context defining, data processing purpose, its</td>
</tr>
<tr>
<td>legitimate and data categorization treated</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Risk identification and risk identification</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Quantitative and qualitative analysis by the CDI</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Two instances in the ISDP where risk measures are</td>
</tr>
<tr>
<td>identified</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>The recording and reporting activity in the ISDP</td>
</tr>
</tbody>
</table>

and success of the product in question. It is identified that the objective would be to introduce guidelines that would explain where missing RM activities would be inserted. The GSMR proposes several activities that "are required for goal-driven risk management" [25], the first activity is initialise goal-driven RM as mentioned before in this activity three transaction kinds were identified T1-scope defining, T2-context establishing and t3-risk criteria defining. [1] [3] The next activity is "identification and modelling of obstacles", as mentioned before, in this activity one transaction kind was identified T4-risks identifying. [1] [3].

The following activity is Assess risks, in this activity three transaction kinds were identified T6-risks priority assessment, T7-risks probability of occurrence assessment and T8-risks impact assessment. [1] [3]

The final activity is treat and monitor risks, as mentioned previously, the identified transaction kinds were T12-risk responses strategies selecting, T13-actions developing, T17-implementation of risk responses monitoring and T18-risk management process effectiveness evaluating. [1] [3]

Table 4.2: GSRM implementation in the data model

<table>
<thead>
<tr>
<th>An empirical study on the implementation and evaluation of a goal-driven software development risk management model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Study 2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Initialises goal-driven risk management</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Identify and model goals</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Identify and model obstacles</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Assess risks</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Treat and monitor risks</td>
</tr>
</tbody>
</table>

As identified in the table 4.2 the data model finds similarities between this IT RM process and the
one proposed by the ontology, however, there is one activity presented in the GSRM process that is not mappable by the data model, this is identify and model goals. The GSRM IT RM process is missing risk owner, shareholder and contingency plan arguments, these arguments come from the missing transaction kinds identified in section 3.2.2.

4.2.3 Case Study 3

As used in section 3 of chapter 3.1. In the third case study, adapted from the article “Introducing OSSF: A framework for online service cybersecurity risk management” [26] a new framework for online security RM services is proposed with the particularity that can be used by service providers and consumers. This framework is called Online Services Security Framework (OSSF). The RM process is proposed in accordance with the ISO/IEC 27005:2011 standard. The OSSF proposes an IT RM process with the following activities: The first activity is General threat scenarios, this activity does not correspond to any activity in the ontology. The next activity is Specific threats identification which, in this activity, no similarities were recognized with the process proposed by the ontology. The following activity is Risks identification and assessment, four transaction kinds were identified in this activity T4-risks identifying, T6-risks priority assessment, T7-risks probability of occurrence assessment, T8-risks impact assessment. [1] [3] The subsequent activity is the risk treatment, one transaction kind was identified in this activity T12-risk responses strategies selecting. [1] [3] Identification of suitable tasks is the following activity, in this activity the T13-actions developing transaction kind was identified. [1] [3] The next activity is the tasks prioritization, in this activity there were not identified transaction kinds. Tasks execution is the following activity, in it one transaction kind was identified in this activity T17-implementation of risk responses monitoring. [1] [3] The last activity in the process is Review of results in this activity, one transaction kind was identified T18-risk management process effectiveness evaluating. [1] [3]

As identified in Table 4.2 the data model finds similarities between this IT RM process and the one proposed by the ontology, however, there are three activities presented in the OSSF process that are not mappable by the data model, these are General threat scenarios, Specific threats identification and tasks prioritization. The OSSF IT RM process is missing risk owner, scope, context, criteria, shareholder, risk source and contingency plan arguments, these arguments come from the missing transaction kinds identified in section 3.2.2.

4.3 Conclusion

In this assessment and taking into account the assessment of the grammatical deficiencies of the conclusions drawn in chapter 3. The identification of transactions enclosed in others will allow establishing the relationships between the various tables produced to allocate the data. The objective will be to
Table 4.3: OSSF implementation in the data model

<table>
<thead>
<tr>
<th>Case Study 2</th>
<th>An empirical study on the implementation and evaluation of a goal-driven software development risk management model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Risk</td>
</tr>
<tr>
<td>Level 2</td>
<td>General threat scenarios identification</td>
</tr>
<tr>
<td>Level 3</td>
<td>Specific threats identification</td>
</tr>
<tr>
<td>Level 4</td>
<td>Risks identification and assessment</td>
</tr>
<tr>
<td>Level 5</td>
<td>Risk treatment</td>
</tr>
<tr>
<td>Level 6</td>
<td>Identification of suitable tasks</td>
</tr>
<tr>
<td>Level 7</td>
<td>Tasks prioritization</td>
</tr>
<tr>
<td>Level 8</td>
<td>Tasks execution</td>
</tr>
<tr>
<td>Level 9</td>
<td>Review of results and benefits of finished tasks</td>
</tr>
</tbody>
</table>

represent the mapping of the case studies in the data model, and the use of this model will make its implementation easier and more agile.

- In the first case study, the stayaway covid application, in the IADP [24], as stated before does not propose a new IT RM process. In this case study, it is verified that all activities can be implemented in the data model.

- In the second case study, as previously mentioned GSRM [25] proposes a new framework with clear guidelines on how to implement IT RM. This process possesses five activities. During the case study implementation, it was verified that the activity of Identify and Model goals cannot be implemented in the data model, which means that the IT RM process proposed by the ontology is unable to map this activity in its process. Which could mean that the activities proposed in the process and the transaction kinds are not enough.

- In the third case study, OSSF [26] proposes another IT RM process, as mentioned above, this process follows the ISO 27005:2011 [27], the analysis of this activity, when implemented in the data model, verifies it turns out that three of the activities are not possible to implement using arguments that were implemented in SQL. This may mean that the activities and transaction kinds proposed in the process are not enough.
Developing a maturity model

Contents

5.1 Development process .................................................. 51
5.2 Maturity model validation ............................................. 52
5.3 Conclusion ............................................................... 61
5.1 Development process

When concerning maturity it is defined as “an evolutionary progress in the demonstration of a specific skill or in the achievement of an objective from an initial state to a desired final state” [17], in this case the specific skill would be the ability to effectively manage the various IT risks and how they optimize the value associated with their IT investments. Maturity models are responsible for defining a number of levels at certain stages of maturity, this levels outline characteristics associated with different stages of maturity [9], they also set the necessary criteria for a continuous progression of the IT RM capability of a given organization. The maturity levels are organized from an initial level of lower capacity towards IT RM, to an advanced level corresponding to the state of the art in IT RM. [4] According to Fraser and Gregory [19] there are six basic components of maturity models, which are a certain number of levels, a descriptor for each level, a generic description or summary of the characteristics of each level, a number of activities for each dimension, a description of each activity as it might be performed at each level of maturity. According to the maturity model proposed by Proença, Borbinha and Vieira [4] there are six maturity levels, one of which corresponds to level zero meaning that there is no RM process within the organization. The defined maturity models are:

- Level 0 - Non-existent RM
- Level 1 - Initial RM
- Level 2 - Managed RM
- Level 3 - Defined RM
- Level 4 - Quantitatively Managed RM
- Level 5 - Optimizing RM

There is another maturity model proposed by Carcary [9] which has different names to the different levels (1 - Initial, 2 - Basic, 3 - Intermediate, 4 - Advanced and 5 - Optimising), however, they are very similar regarding the classification of the different levels. To make the transition from level 0 to 1 the organization needs to implement basic RM tasks and it "needs to be aware that a RM process is needed as a relevant function of the organization” [4], level 1 has a process that just touches the surface of IT RM, meaning “the organization does have a perception of the need for a risk management process” [4], it is said that organizations at this level apply some RM activities with ad hoc procedures and almost always reactively instead of preventively, thus, the results obtained depend more on the competences of the people in the organization than the use of an actual IT RM process. Using the maturity model proposed by Carcary [9] it is also said that there are no formal processes meaning that there is an ad hoc management of IT. Regarding level 2 there must be an established planning of the RM activities to be
carried out, as well as the establishment of a policy regarding RM defined by the organization together with the stakeholders, however it is said that "despite this efforts RM ends up being influenced by the repetition of actions that have worked in the past instead of formal process" [4] meaning that there are still some flaws in establishing a proper RM process across the organization with clear responsibilities and resources. In the transition from level 2 to 3 it is necessary to have an IT RM process "characterized, understood and described in standard procedures, tools, and methods", that is, there is a formalized process and RM is integrated into all organization procedures. Revisions are required periodically to refine both RM policy and the actions taken. The considerable difference between level 3 and the previous one is consistency across the organization and the availability of IT RM training. Regarding maturity level 4, the organization measures quantitatively and statistically the effectiveness of the IT RM process [4] guaranteeing the IT RM process's validity [9]. The fifth and final level is the optimization process through the results obtained from the assessment of the previous level so that risk management is considered a strategic tool. [4] According to Carcary, organizations at this maturity level ensure continuous refinement and updating of both the IT RM process and its policy. [9]

Table 5.1 describes the various levels of risk management maturity that were previously mentioned, as well as their impact on business value and how they are related. Table 5.1 demonstrates the levels that make up the maturity model, the characteristics necessary to achieve them are also summarized, as previously described.

<table>
<thead>
<tr>
<th>Maturity model</th>
<th>Mentioned activities</th>
</tr>
</thead>
</table>
| Level 1        | - There is a risk management report  
                 - Mostly ad-hoc and reactive IT RM activities |
| Level 2        | - People and resources available to IT RM  
                 - Results dependent on people instead of a process |
| Level 3        | - An owner is assigned to each of the risks  
                 - There is a communication and consultation plan  
                 - The organization establishes the context criteria and objectives  
                 - The organization identifies the risks, their sources and priority  
                 - All IT RM activities are monitored and reviewed |
| Level 4        | - Process quality and performance objectives  
                 - Quantitative management measures and analytic techniques  
                 - Performance Baselines and Analysis |
| Level 5        | - Potential improvements identification  
                 - Improvement effects evaluation |

Table 5.1: Maturity model levels represented with their respective activities [4]

5.2 Maturity model validation

Table 5.1 shows the maturity model as well as its levels and the activities associated with each one. According to [4] to move from one level to the next it is necessary to fulfill all the criteria of the current
level, which means that "this maturity model follows a staged approach." Climbing the said stages will ensure the IT RM process will be increasingly optimized and clearly defined. Taking into account the description made in table 5.1 and knowing that level 1 is characterized by organizations that possess the perception that it is necessary to have an IT RM process, however, despite this perception the results are unpredictable since they are dependent on the skills of people in the organization, rather than by applying an IT RM process. Thus, making use of the data model presented above, in figure 5.1, the tables and variables used to characterize this level are described. At this level, the organization only establishes the risk, its impact and someone will define a response to the impact caused. This risk identification will only be done reactively after the consequences.

Figure 5.1: Level 1 featured in the data model.

At level 2, as mentioned above, there is already an effort to establish IT RM activities and people and resources are made available to deal with risks, however, activities will often be reactive rather than proactive. In the data model to move to level 2, organizations will have to identify an owner for each risk and also record and carry out the actions that will be taken in response to it. Figure 5.2 shows changes in the data model, with the introduction of a risk owner and the registration of actions to be carried out to respond to the impact of the threat.
In the transition from level 2 to 3, as can be seen in Figure 5.2, the organization will already establish the scope, context and criteria. From these, the risks are identified as well as their sources, priority and owners. The priority of each of these risks will be calculated based on the probability of happening and the impact that it may have if it happens. Based on the priority of each risk, a plan is identified that contains the actions that will have to be taken to mitigate or minimize the perceived risks.
At level 4 as stated above, the organization quantitatively and for statistical purposes, registers the effectiveness of the IT RM process, that is, there is a concern about the validity of the procedures used and these start being a strategy tool. Thus, the considerable difference in the transition from level 3 to 4 is the introduction of reviews about the effectiveness of the activities and measures implemented in the IT RM process.

Figure 5.4: Level 4 featured in the data model

In the transition from level 4 to 5, the substantial difference is the continuous improvement of the process taking advantage of the effectiveness review. This type of organization is always innovating and developing its IT RM process, thus, organizations that are at this level will inevitably be developing scientific contributions towards IT RM. The differences between level 4 and 5 can be seen in figures 5.4 and 5.5.
5.2.1 Case Study 1

The STAYAWAY COVID app is a contact tracing system, using personal mobile devices, which has been developed in the context of the national health emergency resulting from the COVID-19 pandemic. This application served as the basis for establishing the maturity model and the arguments that make up the tables. In the document "Impact Assessment on Data Protection (IADP)" [24], the various application data protection's risks are identified and analyzed, as well as the diverse activities that allow the management of such risks. In this section the IT RM model presented by the IADP will be evaluated using the proposed maturity model. The scope and context of data processing is established, the purpose of its processing, the legitimacy of its purpose, the category of data that are the target of treatment, and someone is designated as treatment's responsible. Consecutively there are two instances where the risks are identified, one of them using the Confidentiality, Integrity, Accessibility (CIA) triad. The CIA triad is therefore identified risks are analyzed establishing their likelihood and their impact. Risk mitigation measures are consequently identified. The document goes in-depth about three major risk mitigation strategies and also establish responses to the CIA triad. "The risks identified can be considered, in general, as satisfactorily mitigated, by counterbalancing them with organizational and technical measures proportionate to the impact and probability of occurrence of the identified risks". "The regular review of this impact assessment proves to be essential as a control and monitoring measure, safe-
Table 5.2: Stayaway covid application assessed in the maturity model

<table>
<thead>
<tr>
<th>Stayaway covid’s IT RM Process</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope and context defining, data processing purpose, its legitimacy and data categories treated</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk identification and CIA triad analysis</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quantitative and qualitative analysis by the CIA triad</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk identification and CIA triad analysis are identified</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>In the IADP there is a statement saying the risks were satisfactorily mitigated</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The recording and reporting activity is the IADP itself</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Guarding the need to implement other measures to deal with risks detected in the meantime during the use phase, whether in the course of tests or already with general adoption by the population. Once the activities have been identified, we proceeded to the maturity assessment based on the proposed model. This assessment can be seen in Table 4.1. The arguments that were validated in the model were identified in the IADP documentation.

In Table 5.2 it can be seen the arguments that belong to the different maturity levels and how the stayaway covid applications uses each of them in its activities.
Table 5.3: GSRM assessed in the maturity model

An empirical study on the implementation and evaluation of a goal-driven software development risk management model

<table>
<thead>
<tr>
<th>Case Study 2</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Impact</td>
<td>Impact</td>
<td>Impact</td>
<td>Impact</td>
<td>Impact</td>
</tr>
<tr>
<td>T1- scope defining</td>
<td>T2-context establishing</td>
<td>T3-risk criteria defining</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T4-risks identifying</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T6-risks priority assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T7-risks probability of occurrence assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T8-risks impact assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T12-risk responses strategies selecting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T13-actions developing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T17-implementation of risk responses monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T18-risk management process effectiveness evaluating</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In Figure 5.6 it is possible to verify the activities of the IT RM process of the stayaway covid application and its completeness at each maturity stage. Observing the distributions of the various levels for each activity, it is possible to establish guidelines the operation should follow, to reach a certain level of maturity.

5.2.2 Case Study 2

As used in section 2 of chapter 3.1. The second case study, retrieved from the “An empirical study on the implementation and evaluation of a goal-driven software development risk management model” [25] we have a case that aims to develop a software product to satisfy market demand as quickly as possible, therefore allowing a competitive advantage to the company, the case proposes a “Goal-driven Software Development Risk Management Model (GSRM)”. It is, however, identified that there are many uncertainties and risks at all stages of development, these will have a considerable influence on the uncertainty and success of the product in question. It is identified that the objective would be to introduce guidelines that would explain where missing RM activities would be inserted. The GSRM proposes several activities that “are required for goal-driven risk management” [25], the first activity is initialise goal-driven RM as mentioned before in this activity three transaction kinds were identified T1-scope defining, T2-context establishing and T3-risk criteria defining. [1] [3] The next activity is “identification and modeling of obstacles”, as mentioned before, in this activity one transaction kind was identified T4-risks identifying. [1] [3]. The following activity is Assess risks, in this activity three transaction kinds were identified T6-risks priority assessment, T7-risks probability of occurrence assessment and T8-risks impact assessment. [1] [3] The final activity is treat and monitor risks, as mentioned previously, the identified transaction kinds were T12-risk responses strategies selecting, T13-actions developing, T17-implementation of risk responses monitoring and T18-risk management process effectiveness evaluating. [1] [3]
In Figure 5.7 it is possible to verify the activities of the IT RM process of the stayaway covid application and its completeness at each maturity stage. Observing the distributions of the various levels for each activity, it is possible to establish guidelines the operation should follow, to reach a certain level of maturity.

5.2.3 Case Study 3

As used in section 3 of chapter 3.1. In the third case study, adapted from the article "Introducing OSSF: A framework for online service cybersecurity risk management" [26] a new framework for online security RM services is proposed with the particularity that can be used by service providers and consumers. This framework is called Online Services Security Framework (OSSF). As stated before the activities that compose the IT RM process are: The first activity is General threat scenarios, this activity does not correspond to any activity in the ontology. The next activity is Specific threats identification which, in this activity, no similarities were recognized with the process proposed by the ontology. The following activity is Risks identification and assessment, four transaction kinds were identified in this activity T4-risks identifying, T6-risks priority assessment, T7-risks probability of occurrence assessment, T8-risks impact assessment. [1] [3] The subsequent activity is the risk treatment, one transaction kind was identified in this activity T12-risk responses strategies selecting. [1] [3] Identification of suitable tasks is the following activity, in this activity the T13-actions developing transaction kind was identified. [1] [3] The next activity
Table 5.4: GSRM assessed in the maturity model

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>General threat scenarios identification</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specific threats identification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risks identification and assessment</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk treatment</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification of suitable tasks</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tasks prioritization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tasks execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review of results and benefits of finished tasks</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

is the tasks prioritization, in this activity there were not identified transaction kinds. Tasks execution is the following activity, in it one transaction kind was identified in this activity T17-implemention of risk responses monitoring. [1] [3] The last activity in the process is Review of results in this activity, one transaction kind was identified T18-risk management process effectiveness evaluating. [1] [3]

Figure 5.8: OSSF’s IT RM process maturity assessment
In Figure 5.8 it is possible to verify the activities of the IT RM process of the stayaway covid application and its completeness at each maturity stage. Observing the distributions of the various levels for each activity, it is possible to establish guidelines the operation should follow, to reach a certain level of maturity.

5.3 Conclusion

In this third assessment, the completeness of the IT RM process proposed by the ontology was tested using three case studies. This analysis constitutes the third assessment employing the IT RM process and its transaction kinds, as well as the third artifact demonstrated in the DSRM. Observing the distributions of the various levels for each activity, it is more fascinating to establish completeness in terms of maturity levels of a given organization rather than establishing a certain level for an organization’s IT RM process. Thus establishing the guidelines that an organization would have to follow to obtain a certain maturity level in that particular activity. In other words, with this model, it will then be possible to establish an evolution reference or a path to achieve certain maturity goals at the IT RM level.

- In the first case study, the stayaway covid application, in particular the IADP [24], takes advantage of some framework methodologies proposed by the ISO 3100:2009 standard [5]. The first activity establishes scope and context defining, data processing purpose, its legitimacy and data categories treated, as can be seen on fig 5.6 this activity does in only covered in levels 3, 4 and 5. and CIA triad analysis, Quantitative and qualitative analysis by the CIA triad and the IADP identified risk measures, these activities are vastly covered in the proposed maturity, which means that the maturity level in this activity is relatively high. In the last activity of this process, it is verified that it is not mapped by maturity level 1, but is covered in all other levels.

- In the second case study, the GSRM [25] there are five activities, and in the figure 5.7 it can be seen that one of these is not mapped by any maturity level, which was expected since this activity it was not implementable in the data model presented above. It is also verified that the Initialise goal-driven risk management activity cannot be mapped to maturity levels 1 and 2, which means that for its implementation, this process would have to have a maturity level above 3. The remaining activities of the process show high percentages of mapping at different maturity levels.

- In the third case study, the OSSF [26] as expected by the implementation in the data model, the activities general threat scenarios identification management, specific threats identification, and task prioritization are not enabled to be mapped in the established levels as can be seen in figure 5.8. However, all other activities are subject to mapping at all maturity levels.
6

Conclusions

Contents

6.1 Conclusions ................................................................. 65
6.2 Limitations and Future Work ........................................... 66
6.1 Conclusions

The aim of this thesis is the development of an IT RM process maturity model. This will be employed as a tool to assess the completeness of each IT RM activity of a given organization against an IT RM process composed of the most popular activities in the available literature on this subject. This completeness assessment, more than establishing a value that originates a maturity level, allows the establishment of a map for an evolutionary process in terms of IT RM maturity, that is, this model will allow the establishment of guidelines to achieve the goals intended by a particular organization. This thesis also followed an evolutionary process, as suggested in section 1.3, divided into three assessments:

- The first assessment of the completeness of this ontology was argumentative, using three duly detailed case studies and comparing transaction kinds and activities that were or were not present, establishing deficiencies between the ontological constructs and the grammatical constructs [2]. It was detected that the process proposed by the ontology was not fully mapped in all cases, which may suggest a lack of completeness.

- The second assessment, using the same three case studies, consisted of implementing the ontology, translating ontological elements into a data model that will streamline and optimize the comparison process with other IT RM processes. The ontological elements that will be passed as arguments in the data model are those considered necessary to fulfill all transaction kinds identified in the ontology. This implementation was achieved through the relationships between transactions identified in the ontology. [1] [3]

- The third and last assessment takes the data model produced in the previous artifact, producing a maturity model divided into levels, each level will present various arguments from the data model, as the maturity level increases, the number of arguments also increases. The maturity model produced uses other maturity models [4] [9], mentioned above, as a basis for this, a base with a proven representation with the necessary levels is established. The maturity model proposal allows establishing a path that organizations can follow if they want to reach a certain maturity level in terms of IT RM.

This work allowed the evolution of an idea of evaluating the completeness of a given IT RM process through a proposed process that contains the most popular activities in the literature, which evolved from a manual assessment to the establishment of levels and guidelines that will allow greater ease in implementing the ontology in a tool, making the completeness assessment process more agile and faster. Accepting the ontology used as the basis of this work, these data and maturity models will allow a simplification and clarification of IT RM and its use, increasing the probability of a successful implementation of an IT RM process in a given company.
6.2 Limitations and Future Work

Initially, it was devised that the IT RM process proposed by the ontology would be implemented in a real organization to assess its completeness, with the results obtained it would be possible to validate whether the ontology achieves the expected objectives by comparing these with the results obtained by the implementation. However, due to the restrictions caused by the covid-19 pandemic, these assessments were made based on case studies, which, despite allowing the comparison between the various processes, does not make their validation as palpable as would be expected.

Another limitation was the use of the DEMO since it is not applicable to any type of ontology, another limitation is the specific notation of this methodology since understanding is not facilitated for those who are unfamiliar with the notation. The implementation of the data and maturity models also produces limitations in terms of implementation, since decisions were taken to establish arguments and levels that would facilitate the implementation in the respective model.

In the future, it is expected that this data model (which was later implemented in the maturity model) will be implemented on the ATLAS platform.\(^\text{1}\), this will allow the automation of the comparison between the maturity model and a given case study, enabling the mapping of the IT RM process proposed by the ontology in the process outlined by the organization under study. It will therefore be necessary to select the case studies carefully, as they have to be detailed enough to make their evaluation possible. The ATLAS platform will make it possible to compare different blueprints or to compare the same blueprints over time. This will create multiple instances of it in the database, which will allow instantiating different cases within the meta-model, establishing concept differential, and identifying concepts that are or are not covered. ATLAS will invariably receive ontological elements such as the network of transactions and actors at the construction model level, as shown in figure 2, the objective will be to create the ability to say that those ontological elements are the ones that correspond to the initial ontology \(^\text{[1]}\) \(^\text{[3]}\) and to outline from case studies which elements are in excess or lacking in each organization’s IT RM process, to optimize the ontology IT RM process.

This comparison will also aim to determine the organization’s maturity level, establish a path to the maturity that the organisation can follow and establish the differences between both processes. It will be thought-provoking to establish these differences, since it may be verified that it is fact an activity that is missing in the ontology, which may make it more complete. This comparison on the ATLAS platform will be possible by implementing blueprints. A blueprint is a view on the meta-model, in the analyzed case 1, it would be how the STAYAWAY Covid app’s IT RM process compares to the meta-model.

\(^\text{1}\)https://www.linkconsulting.com/what-we-do/products/atlas8/
Bibliography


68
