UNIVERSIDAD DE NAVARRA

ESCUELA DE INGENIERÍA

Cyber Resilience Operationalization Framework (CR-OF) for SMEs

DISSERTATION

submitted for the Degree of Doctor of Philosophy by

Juan Francisco Carías Alvarez

under the supervision of

Dr. Josune Hernantes and

Dr. Saioa Arrizabalaga

Donostia-San Sebastián, September 2021

Cuanto más vivo, más aprendo.

Cuanto más aprendo, más me doy cuenta de lo poco que sé.

— *Michel Legrand*

Agradecimientos

Es difícil resumir en un par de párrafos lo agradecido que estoy con tantas personas que han hecho posible reunir estos humildes resultados que intento explicar lo mejor posible en esta memoria. Pido disculpas de antemano por lo corto que me quedo en estas palabras, pero hago el intento de llegar a, al menos mencionar, a todas las personas que lo han hecho posible.

Primero, quiero agradecer al departamento de organización industrial, a cada uno de sus miembros. Todos son mis maestros, ejemplos o mentores en alguna parte de mi vida actual. Todos me han visto crecer por los últimos 8 años de mi vida. Todos, en conjunto, son mi segunda familia, mi familia lejos de casa... Gracias por apostar por mí, por darme la oportunidad de estar aquí y por todo lo que me enseñaron y transmitieron durante estos años.

En segundo lugar, me gustaría agradecer a mis directoras de tesis, Josune y Saioa. Gracias Josune por enseñarme rigor en la investigación, por sacar lo mejor de mí, por enseñarme con tanto cariño sin dejar de lado la exigencia que necesitaba para creer que las cosas se podían hacer mejor y para creer en mí mismo. Gracias por aguantar mis buenos y mis malos momentos, mis logros y mis

frustraciones... A ti Saioa, te agradezco tu practicidad, enseñarme a poner los pies en la tierra, ser realista con la investigación y poner las cosas en el plano práctico sin dejar de lado la excelencia y la atención en los detalles. Gracias a ambas por todo el tiempo que me dedicaron, todas las horas invertidas en leer versiones de artículos eternos y densos, por todas las horas en reuniones de tesis, por todo lo que me enseñaron. Gracias de corazón por ser mis mentoras en la investigación, modelos a seguir en mi vida y por esta tesis doctoral que en el fondo no es sólo mía, sino NUESTRA.

También me gustaría agradecer a otras tres personas que, aunque no hayan sido mis directores de tesis, son nombres que de manera recurrente aparecen en mis trabajos y que me han dedicado muchísimo tiempo, me han aportado mucho en mi vida y me han dado importantes lecciones a lo largo de estos años. Estas personas son Sarri, Leire y Marcos. **Sarri**, muchas gracias por ser un gran ejemplo de persona, siempre sonriente, con más razones que nadie para estar estresado, pero nunca mostrando ni una pizca de agobio. Por el contrario, me enseñaste que con una sonrisa, las ganas y priorizando correctamente se puede hacer un poco de todo. A ti nunca te faltó el deporte y la alegría en la vida a pesar de todo lo que tuviste en tus hombros, espero algún día poder ser ese ejemplo para otros. **Leire**, gracias por todas las horas leyendo artículos, por todos los consejos, por ser esa tercera directora de tesis que me ha ayudado tanto a mejorar mis trabajos a lo largo de los años. **Marcos**, gracias por enseñarme a pensar más allá de lo evidente, por enseñarme con tantas historias divertidas las lecciones importantes sobre investigación y sobre la vida. Gracias por tu buen humor y por tanta ayuda durante mi tesis.

Haciendo toda mi tesis y sobre todo escribiendo esta memoria me he dado cuenta que tampoco puedo dejar de agradecer a todos los que me dedicaron su tiempo con entrevistas y casos de estudio. Esta tesis, al final, no deja de ser todo ese conocimiento que me han transmitido y que yo he recopilado, analizado y organizado para estos resultados. Muchísimas gracias en serio por todo ese tiempo que me dieron.

Por otro lado, quiero agradecer a mi familia. Mis padres que han sacrificado tanto por educarme y darme hasta lo último para alcanzar todas mis metas. Mi

hermana por todo lo que me ha inspirado para llegar hasta aquí. Mi abuelita por todas sus oraciones. A todos mil gracias.

Finalmente, quiero agradecer a todos aquellos que han estado ahí siempre para escucharme y apoyarme, que me han ayudado a desconectar y descansar cuando lo necesitaba. A todos ustedes: Mely, Brian, Mónica, Jule, Pérez, Karla. De todo corazón les agradezco todo!

Juanfran Carías Alvarez, Donostia 17/06/2021

Outline

Figures

Tables

Abstract

The constantly evolving cyber threat landscape is a latent problem for today's companies. This is especially true for the Small and Medium-sized Enterprises (SMEs) because they have limited resources to face the threats but, as a group, represent an extensive payload for cybercriminals to exploit. Moreover, the risk of cyber incidents is not only due to cybercriminals but can be evoked from multiple sources such as human error, system failure, etc. In any case, the costs of these cyber incidents are high and can considerably affect SMEs.

On the other hand, the traditional cybersecurity approach of protecting against known threats cannot withstand the rapidly evolving technologies and threats. In this sense, this study claims that cyber resilience, a more holistic approach to cybersecurity, could help SMEs anticipate, detect, withstand, recover from and evolve after cyber incidents. However, to operationalize cyber resilience is not an easy task since it requires technical and strategical knowledge and experience for its broad scope, holistic and multidimensional nature.

Although the current literature regarding the operationalization of cyber resilience has widely covered the actions and areas of knowledge (often called policies and domains) required to operationalize cyber resilience, their prioritization and specific implementation strategies are not clear. Moreover, the differences between the actions suggested among the authors require companies to select one approach and later prioritize these actions. Therefore, it requires decision capabilities, knowledge and experience to know what is best for the company. In SMEs, this knowledge and experience might not be present since in most cases cybersecurity is not the core of their business. Therefore, this study tries to facilitate the cyber resilience operationalization process for SMEs.

To achieve the goal of aiding SMEs in cyber resilience operationalization, this study presents an operationalization framework to help them prioritize the required cyber resilience policies and develop effective strategies to implement them. For this, the study presents a classification with the essential cyber resilience domains and policies required to operationalize cyber resilience in SMEs. Once these policies have been established, it also presents an implementation order for effective a cyber resilience operationalization. Moreover, the study presents example progressions for each policy in a progression model in order for companies to be able to strategize how to implement and later improve the required policies. These results are combined into a self-assessment tool and simulation models that could be used by companies in their decision-making process in order to take into account the findings of this study when operationalizing cyber resilience.

1 Introduction

Currently cyber threats are one of the most important risks companies face. These can cost considerable amounts of money and resources from companies, and they are hard to avoid considering their unpredictable and multi-source nature. This can be even worse in the case of companies with low resource availability such as SMEs, which are also the most abundant type of company in our economic environment. Therefore, there is need for an approach in which companies are safe-to-fail and can, not only try to avoid cyber incidents, but rather be able to overcome them and evolve after them. The cyber resilience approach, which is promising for the needed purposes, requires vast amounts of experience, knowledge, and resources for operationalization. Thus, smaller companies with less experience and resources require a different approach than the ones in the current literature. This research attempts to define a continuous improvement process to aid companies in the cyber resilience operationalization in a systematic and effective way that also relieves them from the need of wide experience and knowledge.

1.1 Overview

Cyber threats are one of the main risks companies face today [1], [2], and they affect a large percentage of companies every year [1]–[4]. Threats to information technologies in companies can be classified into two categories: intentional and unintentional [5], [6]. **Unintentional** threats can be due to:

- Natural disasters that can affect the infrastructure's integrity, like floods, fires, etc.
- Human errors caused by personnel's negligence, like installation of unauthorized software or the use of infected USB drives.
- Equipment failure due to failure in electronic components that can lead to system failure.
- Security failures due to the lack of installation of the protection systems.

On the other hand, **intentional** threats have a malicious actor trying to hinder information systems. Two of the most important examples in recent history of cyber threats are:

- Stuxnet, a malware designed to target the industrial control systems (ICS) to slow down the uranium enrichment plants outside of Natanz (Iran), in order to limit Iran's nuclear weapon production in 2009. To do this, the malware made the centrifuges of the uranium enrichment plant spin faster than they were supposed to, and then slower to break the already fragile machines. The exact number of broken centrifuges in Natanz is unknown, but authors estimate between 900 and 2.000 centrifuges in less than a year [7]. Although Stuxnet was an attack to nuclear plants and it is considered to be the first announcement of cyberwarfare [7], [8], it was a direct attack on an ICS and similar attacks could affect any kind of connected factory. Stuxnet was estimated to cost between 243 billion USD in economic losses and 1 trillion USD [9].
- Wannacry was a ransomware in 2017 that affected several important companies around the world [10]–[13]. Wannacry had a worm component that spread through EternalBlue, a Windows vulnerability leaked from the National Security Agency (NSA) months before the exploit. A patch was released by Microsoft, but as usual, many systems

were not patched, and legacy systems (like the ones with Windows XP operating system) were vulnerable [14]. In less than a week, Wannacry was able to spread into 150 countries and millions of systems [15]. The estimated losses due to WannaCry was around 4 billion USD [16]. Thankfully, the code was not the work of professional since the decryption of files was not automatized and the virus had a kill switch that the British hacker known as MalwareTech discovered accidentally when trying to test the malware in a controlled environment [17].

Cyber threats, such as the ones described, can in some way or another disrupt the normal operations of a company and thus cause economic impacts. The economic damage after a cyber incident comes from different sources: loss of reputation and clients' trust, stopped production or services, loss of intellectual property, fines and contractual payment obligations, etc. [18]–[21]. In fact, the economic impact of cyber incidents can cost between hundreds of thousands of euros to the millions per company and per year only in the European Union (EU) [22]. Globally this economic impact is estimated to be around 6 billion US dollars per year and has been increasing during recent years [23].

In this sense, for smaller companies such as SMEs, a successful cyberattack could be catastrophic. In fact, 66% of the companies in a survey of 250 SMEs reported that they went out of business or had to close for a day or more after suffering a cyberattack [24]. Moreover, SMEs are usually specifically targeted by cyber criminals because they represent significant cumulative payoff (from bank accounts, ransoms, credit cards, etc.) with usually not enough means to cover all of their cyber risks [25], [26]. Being targeted and having poor survival rates to attacks can be worrying since SMEs are arguably the most important group of companies in today's economic ecosystem. This is true, since they represent over 90% of companies in most regions [19], [25], [27] and are crucial to the economic development of these regions due to their creation of jobs [28]–[30]. However, SMEs often have scarce resources [25], [27], [30]–[33], and limited workforce focused on this issue to protect against cyber threats [31], [34] which reinforces their cybersecurity problem.

Moreover, the traditional cybersecurity approach has the intention of being fail-safe and the objective of protecting Information Technology (IT) systems [6]. This approach cannot withstand the ever-evolving environment of the cyber risks and technology because technology is evolving faster than companies can adapt to the new vulnerabilities in their systems [26], [35], [36]. Therefore, the traditional cybersecurity point of view needs to shift into an approach that can deal with rapid changes, that maintains business continuity despite unknown, unexpected and adverse situations, and that is sustainable regardless of the changes in the context [36]. An emerging approach to deal with this problem is cyber resilience. This approach is commonly defined as the ability to anticipate, detect, withstand, recover, and evolve from cyber incidents, from an organizational, technological, and human point of view [6], [37]–[39]. Cyber resilience's main intention, opposite to traditional views of cybersecurity, is to prepare the company to be a "safe-to-fail" system with the objective to maintain business continuity despite any type of adverse situations, including unexpected and unknown ones [6], [36], [37], [40].

However, cyber resilience is not easy to operationalize, because it is a multi-dimensional concept that involves governance, awareness and training, and business continuity management [37], [41], [42] among other dimensions for which SMEs usually do not have assigned resources [31], [34]. In addition, cyber resilience also involves the investment in several policies such as preparing for unknown threats, maintaining business continuity, cooperating with external stakeholders, etc. [41], [43], [44] that were not usually considered in traditional cybersecurity [45], [46]. These added policies are complex since they require strategy, planning, testing, coordinating with external entities, etc. and SMEs usually lack the specialized resources to implement them [25], [27], [31], [32]. In fact, most SMEs ignore the need to implement these policies and have either a reactive attitude towards security or the intent to become "fail-safe" with a traditional cybersecurity approach and adopting several technical and protective measures.

Given the importance of SMEs in the current economic ecosystem [19], [25], [27] and their shortcomings for the implementation of cyber resilience [25], [27], [31], [32], [34], an SME oriented approach to cyber resilience is needed.

Currently, several cybersecurity and cyber resilience aiding documents exist in the literature [41], [43], [47]. However, these are not designed specifically for SMEs since they often include hundreds of specific policies [39], [41], [42], [48] that might not all be applicable for SMEs. Thus, it is relevant to define a cyber resilience operationalization approach for SMEs.

A cyber resilience operationalization approach for SMEs should simplify the process by breaking it down into a set of policies useful for them, a way to prioritize these policies, and a description on how to progress over time to implement them. Moreover, this approach should include means for understanding the interrelationships between the proposed policies since understanding these should help them understand their prioritization and use their circumstances to adapt them accordingly on their own.

1.2 Research questions, objectives and publications

Taking into account the need for specific cyber resilience operationalization approaches for SMEs, the research questions this thesis aims to answer are the following:

RQ1. What are the essential cyber resilience domains and policies for cyber resilience operationalization in SMEs?

RQ2. How should SMEs prioritize cyber resilience policies for an effective operationalization?

RQ3. What are the natural progressions and progression types of cyber resilience policies?

RQ4. How to increase the cyber resilience operationalization decision-makers' awareness?

To answer these research questions, the main objective of this thesis is to define a cyber resilience operationalization framework to aid SMEs in their cyber resilience operationalization process. In detail, the research objectives are the following:

1. Define and enumerate the essential domains and policies required to operationalize cyber resilience in SMEs.
2. Outline a general strategy to prioritize the domains and policies for an effective cyber resilience operationalization.
3. Determine realistic progressions over time for the essential cyber resilience policies.
4. Develop management tools to:
    a. Let SMEs self-assess their cyber resilience level.
    b. Aid SMEs in the prioritization and strategic planning of their cyber resilience operationalization process.
    c. Increase the awareness of decision makers about the importance of cyber resilience operationalization and the consequences of their investments (or lack thereof).

It is worth mentioning that the results of this thesis are gathered in four journal publications and five conference proceedings. Table 1.1 summarizes the contributions of each journal or conference publication to both, the research questions and research objectives. In the table, journal publications are named P1, P2, P3 and P4, while conference publications are named C1, C2, C3, C4 and C5. Further details on the publications are given in the last chapter of this dissertation.

- **P1.** Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access*, *8*, 174200–174221. https://doi.org/10.1109/ACCESS.2020.3026063 Impact Factor: 3.367 (Q2)
- **P2.** Carías, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2020). Cyber Resilience Progression Model. *Applied Sciences*, *10*(21), 7393. https://doi.org/10.3390/app10217393 Impact Factor: 2.679 (Q2)
- **P3.** J. F. Carías, S. Arrizabalaga, L. Labaka and J. Hernantes, "Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs," in *IEEE Access*, doi: 10.1109/ACCESS.2021.3085530 Impact Factor: 3.367 (Q2)
- **P4.** Carías, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2019). Defining a cyber resilience investment strategy in an industrial internet of things context. Sensors, 19(1), 138–150. https://doi.org/10.3390/s19010138 Impact Factor: 3.576 (Q1)
- **C1.** Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2021). The Order of the Factors DOES Alter the Product: Cyber

Resilience Policies' Implementation Order. In Computational Intelligence in Security for Information Systems Conference (CISIS) (pp. 306–315). Burgos, Spain: Springer. https://doi.org/10.1007/978-3-030-57805-3_29

- **C2.** Carias, J. F., Arrizabalaga, S., & Hernantes, J. (2020). Cyber Resilience Self-Assessment and Strategic Planning Tool. In Information Technology in Disaster Risk Reduction (ITDRR) (Accepted). Sofia, Bulgaria: Springer.
- **C3.** Carias, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2018). An approach to the modeling of cyber resilience management. In 2018 Global Internet of Things Summit, GIoTS 2018 (pp. 1–6). https://doi.org/10.1109/GIOTS.2018.8534579
- **C4.** Carias, J.F., Labaka, L., Sarriegi, J.M., Tapia, A. & Hernantes, J. (2019). The Dynamics of Cyber Resilience Management. In 2019 International Conference on Information Systems for Crisis Response and Management, ISCRAM 2019 (pp. 64-75)
- **C5.** Carias, J. F., Iturriza, M., Arrizabalaga, S., & Hernantes, J. (2020). Cyber Resilience Awareness Training Cyber Ranges. In the International Emergency Management Society Conference (TIEMS) (Accepted). Paris, France: Springer.

Table 1.1 Contribution of the publications to the research

		P1	P2	P3	P4	C1	C2	C3	C4	C5
RESEARCH QUESTIONS	RQ1. What are the essential cyber resilience domains and policies for cyber resilience operationalization in SMEs?	X				X				
	RQ2. How should SMEs prioritize cyber resilience policies for an effective operationalization?	X	X		X	X		X	X	X
	RQ3. What are the natural progressions and progression types of cyber resilience policies?		X							
	RQ4. How to increase the cyber resilience operationalization decision-makers' awareness?		X	X	X		X	X	X	X
RESEARCH OBJECTIVES	Objective 1: Define and enumerate the essential domains and policies required to operationalize cyber resilience in SMEs	X				X				
	Objective 2: Outline a general strategy to prioritize the domains and policies for an effective cyber resilience operationalization.		X			X				
	Objective 3: Determine realistic progressions over time for the essential cyber resilience policies		X	X	X					
	Objective 4: Develop management tools to: let SMEs self-assess, aid them in the prioritization and strategic planning, and increase the awareness of decision makers			X	X		X	X	X	X

1.3 Thesis structure

The chapters of the thesis are structured in the following way:

- Chapter 2 presents the state of the art concerning cyber resilience. This section gives an overview on the evolution, definition, and importance of the concept for companies in today's context.
- Chapter 3 explains the different phases of the research methodology followed in order to develop the Cyber Resilience Operationalization Framework (CR-OF).
- Chapter 4 explains the followed development process to result in the Cyber Resilience Operationalization Framework (CR-OF). In this chapter, the partial results of the methodologies described in chapter 3 are explained and discussed. The way these results can be merged into the CR-OF is also explained.
- Chapter 5 explains the evaluation phase of the research to ascertain the completeness and usefulness of the CR-OF.
- Chapter 6 summarizes the main conclusions and limitations of this research and proposes ideas for future research.

2 State of the Art

This section reviews and explores the literature on cyber resilience and cyber resilience operationalization for companies. This research posits that in order to operationalize cyber resilience guidelines that are more specialized for SMEs are required since current available documents are often cumbersome and overwhelming for companies that lack previous experience and knowledge.

First, an explanation of the evolution of the concept of cyber resilience, its definitions and the definition adopted in this research are presented. Then, the challenges of the cyber resilience operationalization in SMEs are discussed. Finally, the main contribution of this research is described.

2.1 Introduction

This research is focused on the concept of cyber resilience and, in particular, its operationalization in SMEs. The concept of cyber resilience is a suitable approach to face the challenges of the current cyber threat scenario [44], [49]. In this sense, operationalizing cyber resilience in companies is needed to thrive in a context where threats evolve fast and seem virtually inevitable [26], [35], [36]. However, operationalization of cyber resilience is far from simple and requires a multidimensional and multidisciplinary approach [38]. In this section, the concept of cyber resilience is explained from the point of view of its evolution and the current cyber resilience operationalization aids available in the literature are discussed.

2.2 Evolution of the Cyber Resilience Concept

The literature presents different views on the definition and concept of cyber resilience. These differences can be explained by understanding the evolution of the concept and its origins. Thus, in this section, this evolution is explained in depth. The following subsections present how the concept of cyber resilience was born from the organic evolution of the information security and cybersecurity concepts. Moreover, the differences between these concepts are presented, and one definition for cyber resilience is adopted for the rest of this research.

2.2.1 From information security to cybersecurity

Since the beginning of the internet, in order to protect systems and the information they contain against threats, companies have developed strategies such that the confidentiality, integrity, and availability of these systems are protected [50], [51]. These three characteristics are known as the CIA triad and are key in a discipline known as information security [40].

In this sense, when information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality; when information is modified in unexpected ways, the result is known as loss of integrity; and when

information is erased or becomes inaccessible, the result is known as a loss of availability [50].

On the other hand, cybersecurity adopts information security and goes beyond it, by protecting more than just the cyberspace, but any of the company's assets that can be reached through the cyberspace [52]. In other words, cybersecurity breaches can also affect the CIA triad, but cybersecurity threats can be out of the scope of this classification [40], [52].

Throughout the history of information and communication technologies, the definition of cybersecurity has evolved considerably. This evolution can be observed, for example, in a literature review by Craigen, Diakun-Thibault and Purse [53] in which they try to give a unified definition of Cybersecurity. The definitions they found in the literature are the following:

- "Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders." [54]
- "Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption." [55]
- "Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on." [56]
- "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." [57]
- "The ability to protect or defend the use of cyber-space from cyber-attacks." [58]
- "The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity, and availability." [59]
- "The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure." [60]

- "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." [61]
- "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." [62]

This evolution and the link of cybersecurity with Information security can be also observed when adding the definition by the European Commission: "Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."[63].

As seen in these definitions, in some cases, the cybersecurity definition includes aspects beyond the technical capabilities of a company such as training or collaboration that are more strategic than technical. However, most of these definitions deal with technical aspects only, and they specifically focus on the preparation or protection against cyber threats. Many authors agree that this is no longer enough, because the rapid evolution of technology, the proliferation of cybercrime and the creativity and motivations of the threat actors make it impossible to protect a company from the perimeters [40], [43], [49], [64]–[66].

2.2.2 From Cybersecurity to Cyber Resilience

Thus, despite the slow evolution of cybersecurity to include strategic aspects into the concept and in order to cover a holistic point of view, the scientific community and entities such as the United States Department of Homeland Security (DHS), the European Union or the World Economic Forum, have adopted the concept of cyber resilience [64], [67], [68].

Resilience is a concept used in many disciplines such as environmental sciences, engineering, and psychology. This concept has become relevant in the fields of crisis and disaster management [69]–[71]. In these fields resilience is

defined as the ability of a system to prepare, absorb, recover and adapt to the effects of a major disaster in an effective manner, and evolve in order to improve its capabilities for future events [72], [73]. Notice that this definition can be adapted according to what is considered as a system, for example, a city, critical infrastructure, organization, or information technology systems.

Resilience has been a natural evolution from the concept of risk management [66], [74]–[76]. Risk management analyses the probability of events and proposes a series of measures to manage and mitigate their effect [77]. However, resilience goes beyond this concept by trying to be prepared for these events and the ones that the company does not expect including their cascading consequences. In other words, resilience provides a holistic vision necessary to develop abilities to anticipate and prevent, in addition to developing and practicing the ability to act in a dynamic, flexible and creative way, developing skills that allow companies to adapt to events and threats of unknown origin and unexpected dimensions [69]. Hence, a resilient system would be capable of preventing the occurrence of a crisis, but, more importantly, it would be able to minimize the impact and return sooner to a normal situation.

Due to the popularity of resilience in other fields of study [78]–[80], and its perfect fit in the purposes of cyber systems (where unpredictable risks and critical outcomes are an everyday matter) the concept of cyber resilience is born.

The concept of cyber resilience goes beyond preparation against threats, risk management or the mere protection of the systems. Instead, it includes aspects such as anticipation, detection, response, recovery, and evolution of the systems [37], [43], [49]. These aspects are known as the cyber resilience lifecycle and are shown in Figure 2.1. Besides, cyber resilience is characterized for not looking after individual systems, but networks of systems. In this sense, cyber resilience underlines that networks cannot be secured by securing one system, but by securing the network of systems, i.e., all of the individual systems involved [6].

Figure 2.1 Cyber resilience life cycle

In the literature, there are several cyber resilience definitions. Some examples of these definitions are:

- "Company's ability to continue to function after it suffers a [cybersecurity] breach and to recover gracefully after even a serious security lapse." [38].
- "Cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events" [6].
- "The ability of systems and organizations to develop and execute a long-term strategy to withstand cyber events" [64].
- "An organizations capability to cope with cyber-attacks" [81].
- "Ability of a process, business, organization or nation to anticipate, withstand, recover and evolve in order to improve their capabilities in the face of adverse conditions, stress, or attacks of the cyber resources they need to function." [37].

As seen in these definitions, some authors consider cyber resilience a part of cybersecurity that is concerned with response and recovery exclusively [38], [81], but others consider cyber resilience a more holistic concept that includes the whole lifecycle (Figure 2.1) and that includes strategic and human processes into cybersecurity [37], [64]. This nebulosity of the cyber resilience concept may be due to the continuously changing cybersecurity concept throughout the past few decades [46], [49], [53], [82]. In this thesis, the latter concept in which cyber resilience is considered to include the complete lifecycle is preferred and thus, the definition given by the Spanish National Institute of Cybersecurity (INCIBE for its initials in Spanish) [37] is considered the most accurate since it

encompasses and adapts the resilience stages into the cyber-context. However, in the cybersecurity context, the inclusion of the detection stage is important since there could be significant amounts of time between the beginning of a cyber incident and its detection [41], [44]. Thus, the definition used for this thesis is the following: "Ability of a process, business, organization or nation to anticipate, [detect], withstand, recover and evolve in order to improve their capabilities in the face of adverse conditions, stress, or attacks of the cyber resources they need to function" [37].

It is important to highlight that using this cyber resilience concept is not agnostic of cybersecurity but rather encompasses it. In other words, for a system to be cyber resilient, it must have defined actions to protect against known cyber threats. This means that cybersecurity must play an important role in the preparation and resistance stages of cyber resilience. Sharkov [40] explains this by defining information security as the protection against "known knowns", cybersecurity as the protection against "known unknowns" and cyber resilience as the protection against "unknown unknowns" (see Figure 2.2).

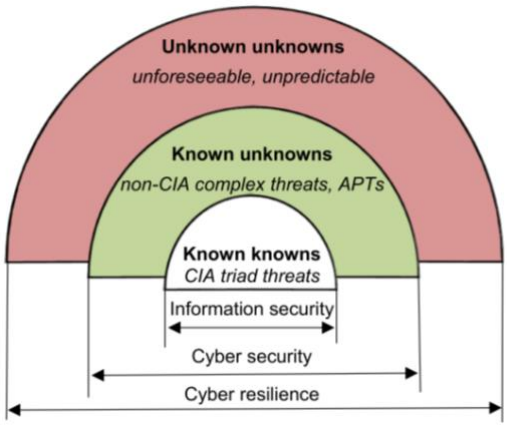

Figure 2.2 Sharkov's graphic definition of cyber resilience

Björk et al. [6] summarize the evolution from cybersecurity to cyber resilience in the 5 main differences that are represented in Table 2.1.

Table 2.1 Five main differences between cybersecurity and cyber resilience

Aspect	Cybersecurity	Cyber resilience
Objective	Protect IT systems	Ensure business delivery
Intention	Fail-safe	Safe-to-fail
Approach	Apply security from the outside	Build security from within
Architecture	Single layered protection	Multi-layered protection
Scope	Atomistic, one organization	Holistic, network of organizations

Considering the cyber resilience concept as described in this section, the following sections of this chapter describe the current problems and previous work on the field.

2.3 The Problems with Cyber Resilience and Cyber Resilience Operationalization

Once the concept of cyber resilience is defined and differed from the cybersecurity concept there are some challenges that arise in its operationalization in companies. First, any company willing to operationalize cyber resilience must change the reactive nature of the traditional concept of cybersecurity into the more proactive nature of the cyber resilience concept. However, companies, and SMEs in particular, are used to being reactive and protective ("fail-safe" approach) [46], [82] towards the implementation of cyber resilience. This makes them prone to being less protected than they might expect from the measures that they have implemented, especially considering that incidents can be provoked by several protective measures failing differently but simultaneously as explained by the complex linear incident model (swiss cheese model) [83]. A visual representation of the model is shown in Figure 2.3. This model has been used in the literature to explain that cybersecurity measures can fail for multiple reasons (human error or latent conditions) and that no measure, nor combination of measures is completely "fail-safe" [84]. Thus, companies not only require cyber resilience operationalization over a traditional cybersecurity one, but also need a systematic and proactive approach towards this

operationalization because adding more protective measures does not always correlate with more security.

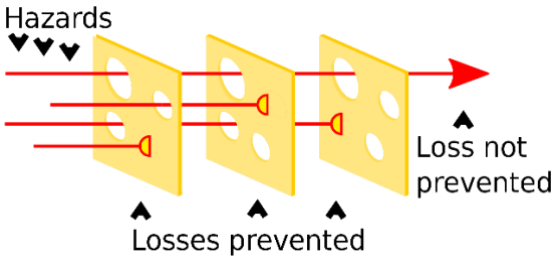

Figure 2.3 Swiss cheese model visual representation

Moreover, the holistic nature of cyber resilience makes it multi-dimensional, and multi-disciplinary requiring several areas of knowledge to be involved [41], [42], [85]. These areas of knowledge include strategic/organizational measures, technical measures and human measures [6], [37]–[39]. This, added to the generalized lack of specialized personnel and resources SMEs dedicate towards cyber resilience [25], [27], [31], [32] makes cyber resilience especially difficult to operationalize for them. Combining a current inertia attempting to become fail-safe [82] and the need for a complex discipline such as cyber resilience to be adopted [44] generates an important barrier towards the systematic operationalization of cyber resilience in SMEs. This is especially highlighted in a context in which SMEs are under constant cyber threat and at the same time lack the human and economical resources to implement cyber resilience [25], [27], [30]–[33].

Therefore, despite the need for implementing cyber resilience in SMEs, these organizations still commonly underinvest in cyber resilience policies because of their lack of awareness about its implications [31], [46]. Besides, SMEs' usually do not have enough means to invest in the required protection, leaving significant risk uncovered [26]. This combination of a lack of awareness and lack of resources make cyber resilience difficult to operationalize since not being aware is also a cause for not investing or underinvesting [86]. Due to this difficulty of implementation, several frameworks, standards, maturity models,

and assessment tools have proliferated in the literature as discussed in the following subsection.

2.4 Previous Work in Cyber Resilience Operationalization

Considering the problems described in the previous sub-section, the current literature tries to ease the process of operationalizing cyber resilience through frameworks, self-assessment questionnaires, standards and maturity models [37], [41], [47], [87]–[92].

2.4.1 Frameworks

A current literature review identified over 200 cyber resilience assessment frameworks [93]. However, these frameworks often include very detailed lists of policies and actions without means for prioritization of these actions or strategies on how to implement each action in the company. Most frameworks can serve as examples of enumeration of policies and areas of knowledge (often found as "domains", "categories" or "controls") that companies should implement in order to operationalize cyber resilience [41]–[44]. For instance, one of the most popular cybersecurity frameworks is the National Institute of Standards and Technology's (NIST's), which lists over 100 policies (called subcategories) in over 30 domains (called categories) to achieve cyber resilience. The document in which these policies are defined explicitly says that they should be selected by the company according to a previous profiling [41], but the framework has no means, instructions or resources on how to do this profiling and how to select and prioritize these policies once the profiling is done.

2.4.2 Metrics

Metrics are also proposed in the literature to aid companies in their cyber resilience operationalization process. Documents suggesting the use of metrics usually list ways to measure an underlying set of policies and domains [39], [48], [85]. For instance, the MITRE corporation's set of cyber resilience metrics contains over 200 metrics. Some examples of these metrics are: Percentage of cyber resources that are properly configured, degree of degradation of mission-

essential functions, average length of time to patch systems, etc. [39]. The MITRE corporation recommends companies to use as few as possible since metrics need to be interpreted and the less they are the easier it is to understand their values [39]. However, this document leaves the selection and prioritization of these metrics to the companies' judgment.

2.4.3 Self-Assessment Questionnaires

Similar to metrics, self-assessment questionnaires often give insight on how the company is now based on an underlying set of policies that companies should follow [37], [88], [92], [94]. Sometimes, these tools can also give suggestions on actions that the company could do to improve its current cyber resilience, but these suggestions are also based on the underlying policies and, therefore, also need prioritization. For instance, the assessment tool proposed by Benz and Chatterjee is based on NIST's framework and its suggestions are to improve the shortcomings of the company by complying with an associated NIST subcategory [92]. This results in a list of subcategories from NIST's framework that are more specific to the company's situation. However, in companies starting their cyber resilience operationalization process this list might still be extensive and require prioritization and customization of those recommendations.

2.4.4 Standards

Standards can also be used to aid in cyber resilience operationalization [87], [95]. The most known example of a standard in this field is the ISO 27000, which can be summarized as a guide on how to make an Information Security Management System (ISMS) and use it to manage information security in a company. Like the ISO 27000, which focuses on information security (a part of cyber resilience [91]), most standards focus on a single aspect of cyber resilience rather than give companies a holistic approach. For companies starting their cyber resilience operationalization, this requires looking for different standards for different cyber resilience domains. Standards also include several actions and processes that should be implemented in the companies that wish to be certified

on that standard. This means that all the policies in a standard should be implemented, but like in the previous approaches, a standard does not give companies starting their cyber resilience operationalization a way to adapt those processes and actions to their own situation. These processes and actions can also require prioritization since standards often have several of these and, depending on the company's circumstances, some may be more important than others.

2.4.5 Maturity Models

The literature also proposes maturity models as an aid for companies to operationalize cyber resilience [47], [88], [96], [97]. Maturity models are in essence sets of characteristics that define a development in a certain entity or field put sequentially in a limited number of stages or levels [98], [99]. Although there are three types of maturity model (capability maturity models, progression models and hybrid models) only capability maturity models can be found regarding cyber resilience in the literature [37], [47], [88], [94]. To briefly define the differences between the types of maturity models, capability maturity models are designed to measure and describe how mature companies' processes are and how embedded these processes are in the company's culture [98]. Thus, they are not a detailed guideline on how to start to operationalize but rather a way of improving or implementing processes that help companies internalize cyber resilience. In practice, this also means that companies require the knowledge to implement these processes and thus the policies and domains supporting them. On the other hand, progression models describe natural progressions and changes in the described characteristic rather than measure how ingrained the processes required for the characteristic to evolve are in the company's culture [98]. In cyber resilience, describing how a policy changes over time has not been done in any of the present maturity models [47], [88], [96], [97]. However, describing the initial form of a cyber resilience policy as well as the gradual evolution of the policy itself over time could aid companies without the experience better understand the policies and how to implement them. Finally, hybrid models are the combination of capability maturity models and progression models [98]. These models could also serve the purpose of aiding

companies at the start of the cyber resilience operationalization process because by definition they would describe the natural progressions of the policies and measure the level of assimilation of the processes required by these policies in the company [98]. However, these are also not present in the current cyber resilience literature [47], [88], [96], [97].

Although it is reasonable to require a profiling of the companies' circumstances or customization of the provided tools, it is also true that many companies will not be able to prioritize correctly or that will require more knowledge, experience and investment in order to do so. Thus, documents that require this customization can overwhelm companies starting their cyber resilience operationalization process and, therefore, there is a need for guidelines and other kind of material to help companies operationalize cyber resilience based on the information already available on actions and policies. Therefore, the closest to guidelines on how to operationalize cyber resilience in the current literature are maturity models. Nonetheless, the current literature offers only capability maturity models [37], [47], [88], [94] which, as mentioned before, require implemented processes to measure how ingrained these are in the company's culture [98].

Progression models, on the other hand, are descriptions of natural progressions over time of characteristics, attributes or policies, which makes their main purpose to provide roadmaps or guidelines expressed as better versions of these policies as the scale progresses [98]. This kind of model can be a better starting point for companies to operationalize cyber resilience, since it describes an implementation from its most basic state, which may be more attainable than achieving a capability or process maturity state when there is no current implementation of the characteristics, attributes or policies in question. Although hybrid models could also be a suitable solution for companies starting their cyber resilience operationalization, a pure progression model is considered better in the context of this study because it is the clearest way to describe the evolution that SMEs should follow without mixing the measurement of the capability of the processes behind those policies [98].

2.5 Research contribution

As shown in the previous subsection, the current documents in the literature meant to aid companies in the operationalization of cyber resilience have mainly focused on the "what" to implement. However, there is a lack of tools for companies to aid them in the prioritization of the policies that the current literature suggests. This lack of prioritization can affect companies in two ways:

1. Companies must select the document that best suits them since they have nuances and differences between each other. This requires the company to have prior knowledge about the existing documents and the differences between them, and enough experience to identify the set of policies that best suit them.
2. Among each document there is a need to prioritize the suggested policies. The implementation of certain policies might be more effective in a particular order, and companies might not think of this when using a list that leaves them full liberty on the order to implement them. For instance, a company might choose to implement security measures before defining what their critical assets are and this might end up costing more money long term. Studies have found particularly ineffective combinations are setting up monitoring systems without proper training [100], or setting up budgets without enough information sharing for situational awareness [86].

In short, prioritization of both, the documents that best suit the company and the timing of the implementation of policies, require resources, experience and knowledge that, as discussed before, SMEs usually lack. On the other hand, strategizing on how to implement each policy can also be a challenge for companies if they lack the knowledge to do so since most of the documents in the literature just list them without expressing their natural progression or ideas on how to start and improve from that base.

Therefore, to aid SMEs in their cyber resilience operationalization, this study proposes the use of a simplified set of domains and policies that contain

the essential actions an SME needs to build cyber resilience. This would minimize the first type of prioritization cited before.

To minimize the second type of prioritization cited before, this study also proposes an effective implementation order for the set of essential policies for cyber resilience operationalization. This implementation order can serve as an initial guide to understand certain relationships and dependencies between the policies but is only proposed as an example that tries to be as general as possible since different company circumstances could lead to different prioritizations.

In addition, the different cyber resilience policies can be implemented in different maturity levels. For instance, it is not the same to have a list of the company's assets in a spreadsheet than having automatic detection of assets that updates a database or repository with the updated inventory. The latter and more sophisticated solution might be overwhelming for a less mature company, but a company that already has an advanced control over their assets might be interested in that solution. Thus, this study also proposes the most common progression types and examples of natural progressions for each cyber resilience policy in the set of essential cyber resilience policies. This result can aid SMEs in two ways: (1) it can help them define initial implementation actions, or (2) it can help them improve their current implementation by giving them specific actions that are common for the more advanced maturity states.

Furthermore, the results mentioned previously as well as many of the documents in the current literature lack an operative way to be transferred to practice (e.g. [41], [43], [44]). Thus, this study also developed a cyber resilience self-assessment tool and proposes the use of system dynamics models as training tools for decision-makers in cyber resilience operationalization.

Thus, the combination of these results composes a cyber resilience operationalization framework (CR-OF) that could contribute to the current literature by aiding SMEs in the strategic planning for cyber resilience operationalization as well as its continuous improvement.

3

3 Research Methodology

This section presents the methodology used to develop this thesis. The methodology comprises five phases: (I) Conceptualization, (II) development of a cyber resilience conceptual framework and implementation order, (III) development of a cyber resilience progression model, (IV) development of simulation models, and (V) the evaluation of the cyber resilience operationalization framework. In each of these phases several research methodologies were applied to gather the required information and develop results that ended up making part of the cyber resilience operationalization framework and its qualitative evaluation.

First, within the conceptualization phase, a literature review was carried out. Then, several semi-structured interviews were used to develop a conceptual framework, an implementation order for the policies described in the framework, a progression model for those policies and simulation models to showcase the interrelationships between those policies. Finally, a series of case studies with SMEs and cybersecurity providers were used to evaluate the cyber resilience operationalization framework.

3.1 Overall research methodology

The research methodology used to develop this study consists of 5 phases: I) a conceptualization, II) the development of a framework and implementation order, III) the development of a progression model, IV) the development of simulation models and V) an evaluation of the results. These 5 phases were combined to develop and evaluate this dissertation's results: a cyber resilience framework, an implementation order for the policies identified in the framework, a progression model for those policies, a self-assessment tool, and a simulation models with interfaces to raise awareness of the decision makers in charge of cyber resilience operationalization in SMEs. Figure 3.1 shows an overview of the complete research methodology and the methods used for the development of each result. The following subsections will describe in detail the process and methods used to develop each phase of the research methodology.

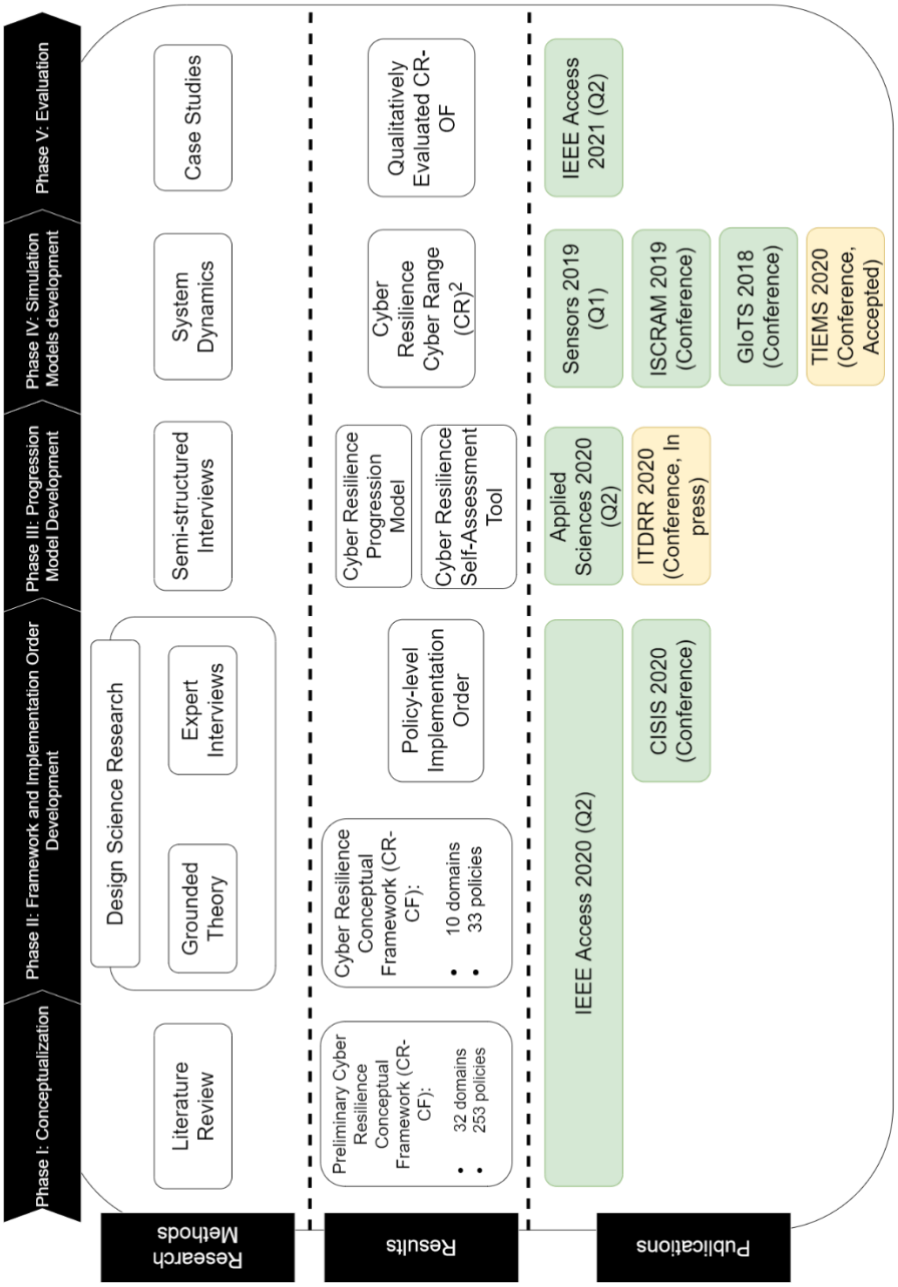

Figure 3.1 Research Methodology Overview

3.2 Phase I: Conceptualization

In order to conceptualize cyber resilience and later develop the cyber resilience operationalization framework for SMEs, a systematic literature review on cyber resilience operationalization documents was performed to select the documents that could aid companies in the implementation of cyber resilience.

Since relevant cyber resilience documents could be provided by intergovernmental organizations (IGOs), non-governmental organizations (NGOs), corporations, and academic literature, the search strategy for this study includes gray literature search in addition to a search in Web of Science (WOS). The keywords used to search were the combination of: *Cyber resilience*, *cyber-resilience*, *cyber resiliency*, *cyber-resiliency*, *cybersecurity*, *cyber security and framework*, *metrics*, *guideline*, *manual*, *agenda*, and *standard*.

The search in WOS generated 88 results and the gray literature search generated 65 results, giving a total of 153 documents. These results were filtered using the criteria described below.

The criteria for a document to be analyzed in this study were:

1. The document explicitly defines a cyber resilience framework.
2. The document defines specific policies, actions, or best practices to aid companies in the implementation of cyber resilience or a dimension of cyber resilience.
3. The document includes Cyber resilience metrics or questionnaires with an understandable conceptual model behind that could be mapped to other frameworks that matched these inclusion criteria.

The criteria to exclude documents from this study's analysis were:

1. Documents that cannot be used by companies because they contain policies meant for other entities (such as countries) and the policies cannot be extrapolated for companies.
2. Frameworks and other types of documents that do not match criteria (2) or (3) from the inclusion criteria.
3. Documents that contain the keywords because they use another cyber resilience or cybersecurity framework, document, set of metrics, etc. but do not present any modifications to the original document.

After searching and applying the criteria, 18 frameworks were selected and analyzed. Table 3.1 shows a list of the 18 identified frameworks that matched these criteria. From the original search, the main exclusions either did not present a set of policies, actions, best practices, or an understandable conceptual model (46 documents) or did not contain any modifications to an original cyber resilience document (51 documents). Other exclusions were documents that despite containing the keywords could not be extrapolated to be used in companies (27 documents) or were duplicated in the different search methods (11 documents).

Table 3.1 List of Analyzed Frameworks

Nº	Year	Author	Document
1	2007	Caralli, R. A. et al.	Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process [101]
2	2009	International Standards on Auditing (ISA)	Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program [95].
3	2012	Information Systems Audit and Control Association (ISACA)	A Business Framework for the Governance and Management of Enterprise IT COBIT 5 [102]
4	2012	Hong Kong Monetary Authority	Cyber Resilience Assessment Framework [103]
5	2012	MITRE Corporation	Cyber Resiliency Metrics [39]
6	2013	Linkov, I. et al.	Resilience Metrics for Cyber Systems [43]
7	2013	International Organization for Standardizations (ISO)	ISO/IEC 27001:2013 [87]
8	2013	National Institute of Standards and Technology (NIST)	Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev. 4) [48]
9	2014	Department of Energy (DOE)	Cybersecurity Capability Maturity Model (C2M2) [47]
10	2016	Carnegie Mellon University	Cyber Resilience Review [88]
11	2016	World Economic Forum (WEF)	A Framework for Assessing Cyber Resilience [44]
12	2016	Carnegie Mellon University	CERT Resilience Management Model (RMM), Version 1.2 [104]
13	2016	Nys, J.	How to Steer Cyber Security with Only One KPI: The Cyber Risk Resilience [85]
14	2017	World Economic Forum (WEF)	Advancing Cyber Resilience: Principles and Tools for Boards [64]
15	2018	National Institute of Standards and Technology (NIST)	Framework for Improving Critical Infrastructure Cybersecurity v 1.1 (NIST Cyber Security Framework) [41]
16	2019	Center of Internet Security (CIS)	CIS Controls V7.1 [42]
17	2019	Pacific Northwest National Laboratory	Buildings Cybersecurity Capability Maturity Model (BC2M2) [94]

18	2019	Instituto Nacional de Ciber Seguridad en España (INCIBE)	Indicadores para la mejora de la ciber resiliencia v 1.1 [KPIs for Improving Cyber Resilience v 1.1] [37]

A comparison between these 18 frameworks is shown in Appendix A. Based on these documents, a series of 32 domains and 253 policies within those categories were identified as a preliminary version of a cyber resilience framework.

3.3 Phase II: Conceptual Framework (CR-CF) and Implementation Order Development

In order to improve upon the preliminary conceptual framework and develop an implementation order to help SMEs operationalize cyber resilience, a variation of the Design Science Research (DSR) methodology was used. DSR methodology is used in this study because its core lies in finding a solution to a problem through the scientifically-based design and evaluation of an artifact (method, model, construct, tool, etc.) [105]–[109]. In this case, there are two outputs or artifacts after using the DSR methodology. The two artifacts would be a framework and an implementation order that can potentially be useful for SMEs to implement cyber resilience.

In this variation of DSR, the grounded theory methodology described previously was used to identify common essential concepts among the cyber resilience frameworks. Afterwards, 11 experts (See appendix B) participated in the study. Six of these experts participated in an iterative process in which the framework improved during four iterations. During these interviews, the framework's policies were also arranged in an implementation order that the experts agreed upon to ultimately define the implementation order that they considered best according to their experience. This implementation order would later aid SMEs in the prioritization of the policies proposed in the framework since experts agreed that it could be ineffective to invest in certain policies without first investing in others. An example they pointed out that is supported in the literature is investing in detection software without the proper training, since the alerts could be false alerts and without the needed knowledge these alerts could make them loose time and resources [100].

Finally, semi-structured interviews with the remaining five experts were used to validate the adequacy of the framework and implementation order to qualitatively evaluate their usefulness in the specific scenario of SMEs.

Figure 3.2 summarizes this described methodology. Each stage of the methodology is explained in the following subsections.

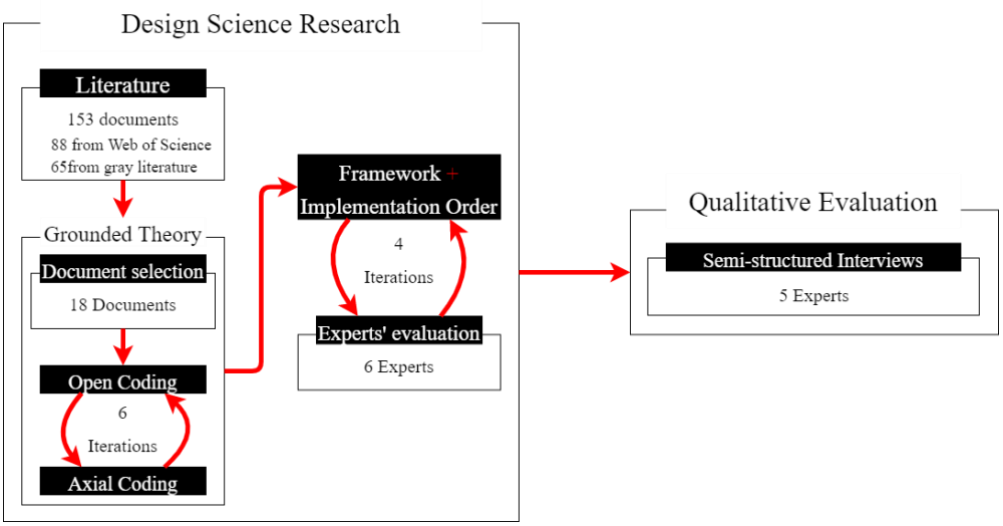

Figure 3.2 Conceptual Framework methodology diagram

3.3.1 Grounded Theory

In order to find a unified approach and a set of essential policies among the 18 cyber resilience documents found in the literature, the Grounded Theory methodology was used. Grounded Theory methodology aims to find new theories from the iterative process of coding and comparing the concepts in the data [110]. Similar to the inductive methodology the Grounded Theory methodology finds particular cases and tries to generalize these cases into the general concepts that govern them [111]. Many grounded theory analysis are based in document analysis [112], [113] using the documents as a mean of finding particular data that through a systematic process of identifying common grounds can be generalized into a theory [110], [112], [113]. In this sense, Grounded Theory methodology requires two stages: selecting documents to analyze and a coding

process to systematically identify common concepts between these documents [110].

In this study, the documents used to start the grounded theory analysis were the 18 documents identified previously.

Furthermore, the systematic identification of concepts and ideas in the documents was made in two phases: an open coding approach followed by an axial coding approach with iterative constant comparison of the codes [114]. Similar combinations of coding techniques within the grounded theory methodology are commonly used, and encouraged by other authors [112], [114], [115].

The open coding approach was used to assign codes, compare, conceptualize, and categorize the available data [114], [116], [117]. In this case, the available data was the policies, domains and concepts in the cyber resilience documents. For this reason, the documents were carefully read, the policies, concepts, and domains were assigned a code and classified into a set of groups based on similarities, and interrelationships. After this, an axial coding approach was used to reorganize categories, find links between them, and synthesize the information as much as possible [114], [118]. In this phase, groups of policies were joined based on their similarity, and certain groups of policies were separated into several groups when the subgroups were very recurrent in the literature.

After six iterations of open and axial coding, the codes were grouped into categories. In the context of this study, these categories have been called "domains" because it is the name given to similar categories in the literature [47], [88]. However, these domains would be equivalent to what is found as "categories", "capabilities" or "controls" in other frameworks [41], [42], [85].

Within the identified domains, concrete actions grouped from different metrics, policies and actions suggested in the documents. These were assigned as the domains' "policies". At the end of the process, an improved version of the framework was obtained with 20 domains and 75 policies. With the iterative development with the experts, these domains and policies were further filtered

and improved to achieve the final result of the CR-CF as will be explained in the next subsection.

3.3.2 Iterative Development

To further improve the framework and develop the implementation order 6 experts were interviewed. The six experts had wide experience in cyber security for companies and were familiar with the cyber resilience concept. The backgrounds of these experts are: one director of an industrial cybersecurity center, one chief operations officer from an industrial cybersecurity center, one data protection officer, one chief information security officer from a medium-sized company, and two cybersecurity researchers.

In this stage, the experts were presented with the resulting framework and were asked to review it and comment on its completeness, structure, and adaptation to SMEs needs. The experts were also asked to order the framework's policies in what they thought would be the ideal order of implementation. Once the comments from the different experts were received and included, the process was repeated until a consensus was reached. This process took four rounds of feedback for consensus to be reached. During these iterations, experts excluded certain domains and policies, grouped others and included the ones they considered were important but not stressed enough in the previous versions. After this process the framework had 10 domains and 33 policies. These policies and domains were also ordered in an example implementation order the experts considered as an effective cyber resilience operationalization implementation order.

3.3.3 Qualitative Evaluation

To evaluate the usefulness of the CR-CF and implementation order, the five remaining experts participated in semi-structured interviews. Semi-structured interviews are a means of data collection for qualitative research useful to gather information about a particular topic or area from the experience of individuals [119]. This set of experts had the following backgrounds: one is an industrial cybersecurity researcher, two of them are CISOs from medium sized companies with many years of experience in that place, one is the CEO of two companies (a

medium-sized family company and a startup he founded) and the last expert is a consultor in a cybersecurity provider.

These experts were presented with the framework and the implementation order to evaluate adequacy of the domains, policies, identified dependencies for the implementation order and asked questions such as: "Do you think the framework includes all the essential cyber resilience domains?", "Do you think the policies for each domain are adequate to implement that domain?", "Do you believe that the dependencies identified in the implementation order are correct and would represent an effective order for cyber resilience implementation?", and "Do you consider the framework could help an SME manager understand how cyber resilience can start to be operationalized?".

With the answers of the experts, the CR-CF was qualitatively evaluated and seemed to be a complete set of essential policies that could aid SMEs in their cyber resilience operationalization process.

3.4 Phase III: Progression Model Development

In the previous phases a conceptual framework (CR-CF) with the essential domains and policies for cyber resilience operationalization and implementation order to prioritize them have been defined. In this phase, the objective is to define a progression model to give companies guidelines on how these policies will evolve over time after a basic implementation. For this purpose, this study carried out semi-structured interviews as a source of qualitative information in order to obtain a cyber resilience progression model. In this particular case, this methodology was used to collect information on the progression of cyber resilience policies from 11 experts of three different profiles: cybersecurity providers (3), cybersecurity researchers (3), and professionals in companies in charge of cybersecurity implementation (5) (See appendix B). The profiles of the four new experts were three cybersecurity providers and one CEO of an SME. These 11 experts were selected due to their wide experience in the field and their profiles were chosen to add the three perspectives on the topic. These three perspectives were chosen because they are considered to be the different stakeholders that could influence the operationalization of cyber resilience in

SMEs. This diversity of backgrounds also reaffirmed the usage of semi-structured interviews as a way to ensure a standardized understanding of the questions and vocabulary in the interview [120].

The interviews were made using the cyber resilience conceptual framework (CR-CF) developed as a previous result as the base to build the cyber resilience progression model. Using these findings, the semi-structured interviews were designed and later quantified and analyzed in order to define how the policies from that conceptual framework progressed over time. The design of the interviews, their development, and their analysis are described in the next subsections.

3.4.1 Interviews' Design and Execution

In order to obtain a progression model from the experts' point of view, the interviews were designed to be a systematic construction of a progression model. To achieve this, all the experts were given a simplified version of the domains and policies (e.g., "make an inventory of assets" instead of "Make an inventory that lists and classifies the company's assets and identifies the critical assets"). These simplifications were made to avoid biasing the perspective of the expert by adding advanced characteristics of the policy within the way of writing it. The table with the domains and simplified policies was given to the experts in a document that served as the interviews' script. This document also contained the definitions for "cyber resilience" and "progression model" as well as the objectives of the interviews, the expected results and the following two-step methodology:

- Step 1: Establish a starting point for each cyber resilience policy. In this step, they were also asked to keep in mind dependencies among these policies and their own experience in order to place these policies on a starting point from a scale of 1–5. Where one is the least advanced, least mature of companies and five the most advanced maturity level. The scale was selected based on other maturity models in the literature, which vary from three to six maturity levels [47], [88], [94].

- Step 2: Describe how these policies progress over the next steps of the scale. For instance, if a policy starts at level three, how the policy manifests in a company at level three, then level four, and finally level five.

In these steps the scale was defined without names for each maturity level to avoid biasing through the usage of names (e.g., if level 5 is called "Optimizing" as in the Capability Maturity Model Integration (CMMI) [121], the actions described in level five would be limited to optimization actions). Other maturity models in the literature also avoid the usage of names for their maturity levels [47], [88].

With this information, the experts were interviewed one by one and the 11 interviews were recorded to ensure their correct transcription. The transcriptions were also sent to each expert in order to double check that their ideas were captured accurately and avoid incorrect recording of data and/or a biased interpretation of what the experts responded. A graphical overview of how the resulting progression model from each expert is shown in Figure 3.3. This is also similar to the final result of this study after the analysis of the interviews described in the following subsection.

Domain	Policy	1	2	3	4	5
Domain 1	Policy 1		Policy starting description	Evolution description at level 3	Evolution description at level 4	Evolution description at level 5
	Policy 2			Policy starting description	Evolution description at level 4	Evolution description at level 5
	Policy 3		Policy starting description	Evolution description at level 3	Evolution description at level 4	Evolution description at level 5
Domain 2	Policy 4				Policy starting description	Evolution description at level 5
	Policy 5		Policy starting description	Evolution description at level 3	Evolution description at level 4	Evolution description at level 5
	Policy 6	Policy starting description	Evolution description at level 2	Evolution description at level 3	Evolution description at level 4	Evolution description at level 5

Figure 3.3 Graphical overview of resulting progression models

During the interviews, the experts commonly asked the following questions:

- If they could start a policy at level five and, therefore, have no evolution. This was allowed as it was considered an interesting statement on the complexity of a policy.
- If policies could stay the same through various levels (or skip them, which was equivalent) and evolve when the level of

maturity was higher (for example, stay the same from 1–3 and change in 4 and 5). This kind of evolution was also allowed since it would allow a realistic view of the progression of a policy.

- If they should try to depict reality or define the best possible scenario. In this case, they were asked to do their best to be realistic but in case they believed a policy is not applied in their context to try to place the policy in an ideal starting point considering the companies' capacities at that maturity level.

To avoid fatigue during the interviews and thus bias due to this fatigue, the interviews were limited as much as possible to one hour and 30 min. The average duration of the interviews was 1 h and 20 min. This was possible because the experts were given the scripts previously and the transcription of their ideas was made after the interview, which permitted the experts to speak freely and without delays.

3.4.2 Analysis of Interview Transcripts

As mentioned in the previous subsection, at the end of the interviews, the transcripts resulted in progression models from the point of view of each expert. To analyze these transcripts, the five-step methodology for analyzing semi-structured interviews suggested by Schmidt was used [122]. These five steps are:

1. Material-oriented formation of analytical categories, which consists of carefully reading and understanding the individual transcripts. In this step, annotations were made on the common concepts found among the transcripts as they were read individually.
2. Assembly of the analytical categories into a guide for coding, which in the case of this study consists of creating categories that summarize the different types of progression identified by the experts. These types of progression were defined by grouping common patterns on the experts' progressions (found on the interviews) and naming these patterns as descriptively as possible.
3. Coding of the material, which consisted of assigning a progression type to each of the policies and progressions from the transcript of each expert. In this step, multiple codes could be assigned to each policy's progression from a single expert.
4. Quantifying surveys of material, which consisted of two parts: (1) determining whether there was consensus on the starting maturity of

each policy and (2) determining whether there was consensus on the progression type for each policy. The process used to determine consensuses is described in appendix C.

5. Detailed case interpretations, which in this context consisted of creating a progression model based on the interpretation of the most common starting point for each policy and its most common progression type (code). In this step, when there was a tie in the starting maturity of a policy the lower maturity was used, and when there was a tie in the progression type a mix of both progressions was used for the construction of the progression model.

A summary of the five-step methodology with the results from each step is shown in Figure 3.4.

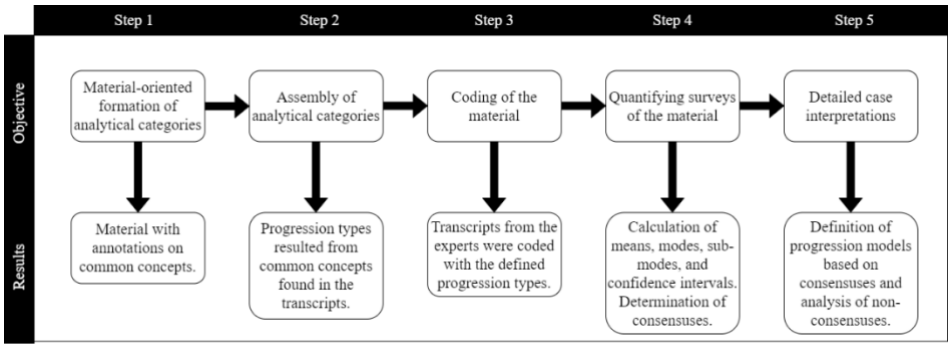

Figure 3.4 Transcript analysis methodology summary

3.5 Phase IV: Simulation Models' Development

Once SMEs have the domains and policies they need to implement, guidelines on how to prioritize them and paths to follow once they implement a basic form of each policy, it is important to understand why these guidelines exist. To raise awareness in this sense and let decision makers understand the consequences of their investments (or lack thereof) System Dynamics (SD) simulation models were developed. SD modelling and simulation has frequently been used to illustrate the dynamics and the trade-offs between different competing decisions and options over time [123]. Thus, the SD simulation technique is also often considered as a safe environment to conduct experiments, test decisions, and observe the consequences on a system [123]. Moreover, one of the SD strengths is its ability to model socio-technical systems and dealing with

the soft variables that are hard to quantify but are often influential to determine the behavior of variables under study [124]. Given the ability to show trade-offs and model mixed numerical and soft variables such as the ones found in cyber resilience operationalization the method is deemed to be appropriate for the purpose of this study.

In order to develop the simulation models for this study a literature approach was combined with the results of the previous expert interviews to obtain the reference modes (behaviors over time or BoT) and the boundaries of the models. This process is summarized in Figure 3.5 and explained in the following subsection.

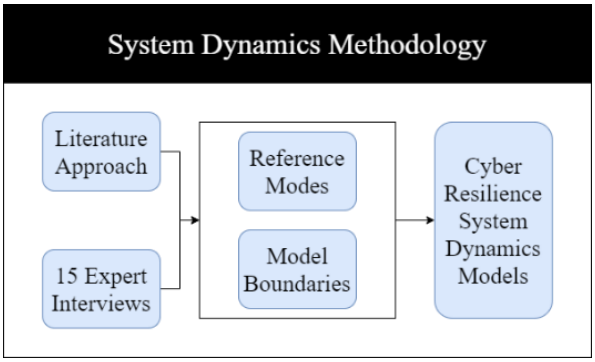

Figure 3.5 Summary of the employed methodology

3.5.1 System Dynamics Modelling

To develop the SD models, in addition to a literature approach, interviews with 15 experts were used to elicit their mental model and tacit knowledge concerning the investment decisions for improving cyber resilience. Out of these experts, five differed from the ones who participated in the previous phases. However, these experts had the same characteristics: wide experience in the operationalization of cyber resilience or they researched in cyber resilience. Using experts' tacit knowledge is a known process in the SD model building, as many SD modelers admit that the knowledge of the stakeholders who actually operate the system is required to structure and parameterize a useful model [125].

The literature approach was used to find interrelationships and known behaviors discussed in the literature. Previous research and the cyber resilience aiding documents discussed in the conceptualization phase were used to find interrelationships between cyber resilience policies and domains. Other articles discussing interrelationships between policies and the importance of certain policies (such as, [86], [100]) were also studied before comparing and contrasting with the experts' opinions on the important relationships and effects of cyber resilience domains and policies.

Later, the information was contrasted with the interrelationships and behaviors described in the 15 expert interviews (See appendix B). The aims of the interviews with the experts for knowledge elicitation were twofold: First, to derive behaviors or reference modes, which is required in the SD method [126] to describe the dynamic of the problems being modeled. Second, to estimate the boundaries or orders of magnitude in the model and the time horizon that would be applied in the cyber resilience model were plausible. The elicitation process was designed to allow the experts drawing the Behavior over Time (BoT) as input for the model to represent the reality. Despite the chart would not be an exact quantitative representation, it is vital to understanding the dynamics of managing cyber resilience [124].

3.6 Phase V: Evaluation

Once the final Cyber Resilience Operationalization Framework (CR-OF) was defined through the previous steps of this methodology, six case studies were carried out to confirm the framework contributes in a complete and useful way to the operationalization of cyber resilience in SMEs. Therefore, these case studies had two main objectives:

1. Determine whether the CR-OF was **complete** or, in other words, if it encompassed all the policies SMEs expect for cyber resilience operationalization.
2. Determine whether the CR-OF was **useful** or, in other words, if SMEs could successfully use the CR-OF to follow the process of self-assessing

their current cyber resilience, decide actions to improve it and prioritize these actions.

For companies to be able to use the CR-OF, the Cyber Resilience Self-Assessment Tool (CR-SAT) was used in a web-based prototype that guided them through the process of self-assessing, deciding improvement actions and prioritizing them. The following sub-section describes the case study methodology, its fit in this context, and its application in this thesis.

3.6.1 Case Studies

The case study methodology is used to explore and study real-life events and their relationships in a detailed context analysis [127]. Due to their nature, case studies explore empirical evidences of the studied phenomena in which causality, interrelationships between the observed variables become apparent [127]. In this sense, a case study might help improve, and evaluate the completeness and usefulness of the CR-OF. This use of case studies is also supported in the literature since case studies can be used to illuminate a set of decisions: why they were taken, how they were implemented and with what results [127], [128].

To avoid biases in the interpretation of the information of the data obtained from the case study, a triangulation of information gathered from different sources was used. This information came from documental evidences, websites, interviews and official documentation (internal reports and plans). This process was used to alleviate the lack that case studies are usually accused of because of the interpretability of the data, and at the same time ensure the reliability of the data gathered [129], [130].

Considering this, the main source of information for the case studies in this article were semi-structured interviews, and this information was contrasted with publicly available information from the companies as well as internal reports provided by the interviewees. Semi-structured interviews are a means of data collection for qualitative research useful to gather information about a particular topic or area from the experience of individuals [119]. In the case

studies conducted for this article, the semi-structured interviews were geared towards the collection of empirical evidences of the current state of each cyber resilience policy in the company to denote the possibility of correctly identifying with the scales used in the tool. These empirical evidences were used to improve the scales and questions with examples that could potentially help future SMEs using the tool to identify with an option with more ease. Moreover, the case studies also had the objective of finding evidences that decision-makers could extract specific actions to improve their cyber resilience from the tool's scales (or their equivalent, the progression model) and prioritize these actions with the help of the tool. The final objective of the case studies was to receive feedback on the overall usefulness of this kind of tool and process.

To fulfill these objectives, contact with the SMEs in these case studies were through one spokesperson who was selected with the criteria of having decision over cyber resilience operationalization in the company. In this way, the person could either respond in a first interview, get informed with the rest of the personnel and respond in a later interview, or delegate the response to the more adequate profile. Using these criteria, six cybersecurity managers (see appendix B) from three different SMEs were interviewed and their companies participated in the case studies. The profiles of these interviewees were: one CTO (chief technology officer) of a 150-employees port logistics company in El Salvador. One CEO (chief executive officer) and financial director of a 200-employees paint, varnish, ink and similar coatings company in the Basque Country, Spain. One CEO of a 30-employee clinical pharmacy organization in Florida, USA. One CTO from a 225-employee machine tool manufacturer from Spain. One CTO from a 150-employee machine tool manufacturer (competitor of the previous company) in Spain. Finally, one CEO of a 50-employee mold manufacturing company in Spain. In these companies, these interviewees were in charge of cyber resilience decision-making.

During the case studies, the companies' spokespersons had to self-assess the company supporting their assessment with evidences, select actions to improve their current cyber resilience operationalization and prioritize these actions according to the implementation order obtained in phase II of the methodology (which was provided to them through the CR-SAT application).

At the end of the case studies, each company's spokesperson was asked to give feedback on the tool, its completeness and how useful they found it when self-assessing, defining their improvement actions and prioritizing them.

Afterwards, based on the results of the case studies, cybersecurity providers were identified as an important stakeholder in the cyber resilience operationalization in SMEs. Therefore, to evaluate their perspective on the usefulness and completeness of the cyber resilience operationalization framework (CR-OF), three cybersecurity providers were also interviewed (See appendix B) and presented with the CR-SAT to see if they considered it a viable option to aid SMEs in cyber resilience operationalization.

3.7 Conclusion

The research methodology applied in this research comprised five main phases: conceptualization, development of a cyber resilience conceptual framework (CR-CF) and its implementation order, development of a cyber resilience progression model, development of simulation models, and the evaluation of the cyber resilience operationalization framework (CR-OF). The conceptualization phase included a literature review of different documents that aid companies in cyber resilience operationalization. Using this information, the development of the CR-CF and its implementation order were developed by systematically finding similarities and underlying concepts in the existing documents to uncover the essential cyber resilience policies, which were also qualitatively evaluated and put into an implementation order by eleven experts. Then, a different group of eleven experts aided with the definition of an initial maturity state and progression types for each of the policies in the CR-CF. Using this information a progression model was developed in phase III. Thereafter, another set of experts was interviewed to develop SD models to simulate the consequences of different prioritizations and investments strategies in cyber resilience policies. These models were later proposed as a valid tool for cyber resilience awareness training, especially for decision-makers. Finally, during the evaluation phase (phase V), the correctness and usefulness of the cyber resilience operationalization framework (CR-OF) were tested in six case studies. Using

these methodologies, the following chapter explains the obtained results and how these results are merged as a useful framework for cyber resilience operationalization in SMEs, the CR-OF.

4

4 Cyber Resilience Operationalization Framework (CR-OF)

This chapter presents the different results that, when used conjunctly, form the cyber resilience operationalization framework (CR-OF). As explained in the methodology section, the results were obtained gradually throughout the different phases of this thesis' development. Therefore, this section presents in a detailed manner these results and how they can be used together as an operationalization framework (CR-OF).

4.1 Introduction

The results of this thesis can be summarized in two groups. The first group is a conceptual framework (CR-CF) with the necessary means to prioritize and implement it, and the second group are operative tools that companies can use to apply the concepts and prioritizations and that way operationalize cyber resilience. The results in the first group are:

1. The cyber resilience conceptual framework (CR-CF) that contains the essential domains and policies that SMEs require to operationalize cyber resilience.
2. The implementation order for SMEs to have guidelines on how to prioritize the domains and policies in the CR-CF.
3. The cyber resilience progression model for SMEs to have guidelines on how each policy can evolve from an initial implementation into mature states.

On the second group, this study presents two tools for SMEs:

1. The Self-assessment tool (CR-SAT) for companies to assess their cyber resilience operationalization based on the progression model and the implementation order.
2. The cyber resilience cyber range $(CR)^2$ that based on the progressions and prioritization of the policies allows SME managers understand the effects of each policy and the effects of their decisions.

Figure 4.1 summarizes these results that constitute the Cyber Resilience Operationalization Framework (CR-OF) and organizes them from most theoretical to most operative (top to bottom).

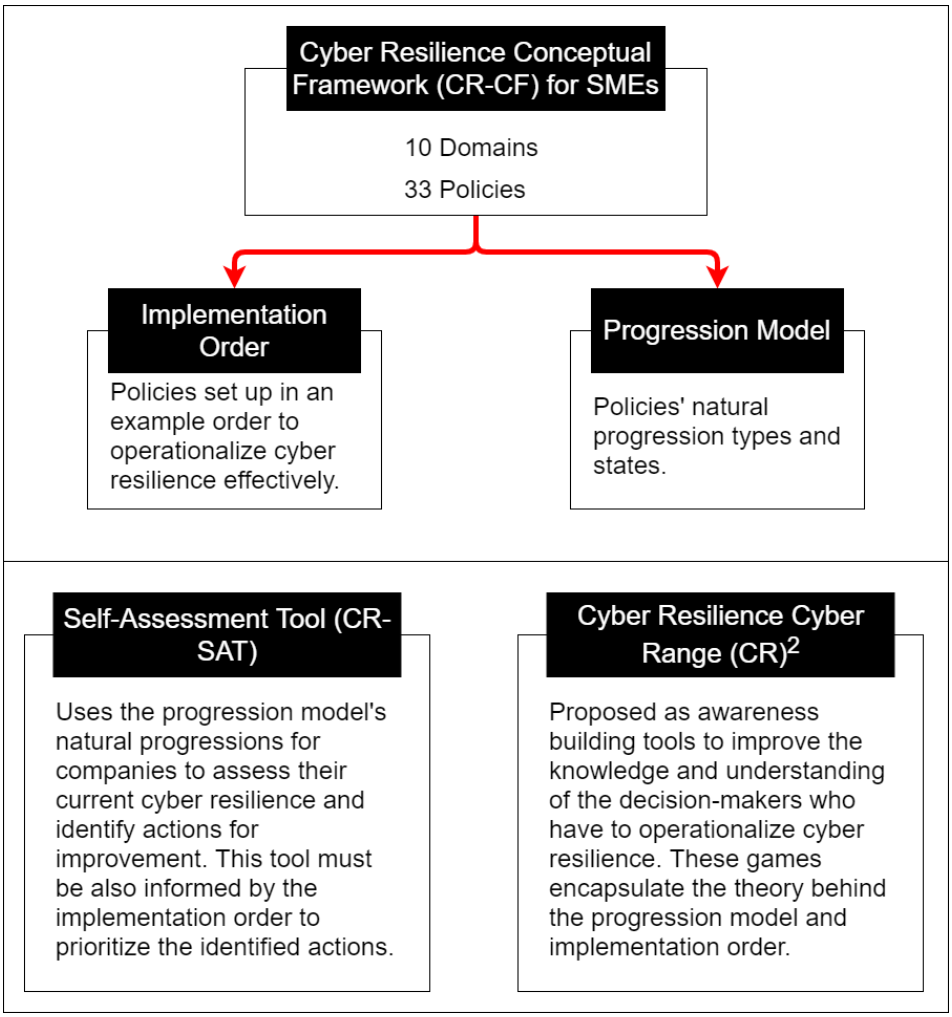

Figure 4.1 Cyber Resilience Operationalization Framework (CR-OF) results summary

4.2 Cyber Resilience Conceptual Framework (CR-CF)

After applying the methodology described in the previous chapter (Section 3.3), cyber resilience has been synthesized into 10 domains and 33 policies for SMEs to follow and implement. As mentioned in the previous section, the policies and domains in this conceptual framework had to appear repeatedly as concepts in the literature and had to be approved by the experts as necessary for SMEs.

At the end of this section, a table with the summary of the CR-CF and a comparison to other frameworks in the literature is given in Table 4.1 CR-CF and other frameworks influences.

In the following subsections the conceptual framework is broken down into its domains and amongst each domain the policies that compose it.

4.2.1 Governance

The reviewed cyber resilience frameworks often reference concepts related to the role of the management in promoting/sponsoring cyber resilience [47], [64], [88], [94], [101]–[103], communicating cyber resilience plans [43], [44], [88], [94], developing a cyber resilience strategy [41], [47], [64], [85], [94], [102], assigning enough resources to develop cyber resilience activities [94], [101], [103], and complying with cyber resilience-related regulation [44], [85], [87], [102], [104]. The CR-CF has grouped this common theme under one domain called "governance" since several of these frameworks explicitly name similar groups under that name [41], [85], [88], [103].

Based on these concepts and the experts' reasoning, the specific policies for the governance domain were summarized as follows:

- Develop and communicate a cyber resilience strategy.
- Comply with cyber resilience-related regulation.
- Assign resources (funds, people, tools, etc.) to develop cyber resilience activities.

Although it is not a specific action and thus it cannot be written as a policy, this domain must stress the importance of the management's awareness, commitment and engagement. In short, the management should lead the initiative in the cyber resilience implementation process [35].

4.2.2 Risk Management

Another group of concepts that was often referenced in the reviewed frameworks and was considered important in the expert's evaluations were the concepts related to cyber risk. These concepts included the systematic identification and documentation of risks [41], [47], [64], [87], [88], [94], [101], [103], [104], the classification of these risks in order to determine priorities [41],

[42], [47], [87], [88], [94], [104], the determination of an acceptance threshold for risk [41], [47], [64], [88], [103], [104], and the development of risk mitigation activities [41], [47], [48], [64], [87], [88], [94], [101], [104]. In the CR-CF, these concepts have been grouped under the "risk management" domain. This title is recurrent in the reviewed frameworks, along with "risk assessment", to group similar concepts [41], [47], [48], [64], [85], [87], [88], [94], [101], [103], [104].

Due to the cited commonly found concepts and after iterating with the experts, the risk management domain's policies were written as follows:

- Systematically identify and document the company's cyber risks.
- Classify/prioritize the company's cyber risk.
- Determine a risk tolerance threshold.
- Mitigate the risks that exceed the risk tolerance threshold.

According to the experts, risk management should consider internal and external risks. This statement is backed up in the literature since many frameworks include the analysis of external risks [41], [47], [88]. The external risks are important to consider in order to implement cyber resilience since viewing the organization as one part of a network of organizations is a key difference between cyber resilience and traditional cybersecurity [6].

4.2.3 Asset Management

Many concepts in the reviewed cyber resilience frameworks referred to the company's assets (hardware, software, and communications). These concepts include creating an inventory of the company's assets [37], [41], [42], [47], [48], [87], [88], [94], [103], [104], creating and documenting a baseline configuration of the assets and a configuration change policy [41], [42], [47], [48], [88], [104], keeping the assets maintained [37], [42], [47], [48], [87], [88], [103], [104], and identifying the internal and external dependencies of those assets [43], [44], [88], [103], [104]. The name of the domain that groups these concepts in this study's conceptual framework (CR-CF) is "asset management" because it is a name commonly used to group these concepts together in the reviewed frameworks [41], [88], [94], [104].

Based on these concepts and the experts' input, the asset management domain of the CR-CF contains the following policies:

- Make an inventory that lists and classifies the company's assets and identifies the critical assets.
- Create and document a baseline configuration for the company's assets.
- Create a policy to manage the changes in the assets' configurations.
- Create a policy to periodically maintain the company's assets.
- Identify and document the internal and external dependencies of the company's assets.

The asset management domain, according to the experts can affect the anticipation stage of the cyber resilience domain. This is because when implemented, asset management can help the company know what to protect and prioritize the protection of critical assets [43].

Asset management also includes the analysis of dependencies from the company's assets with external systems. This is important in order to include the external aspects that are key for cyber resilience [6], [86].

4.2.4 Threat and Vulnerability Management

Other concepts found to be in several of the reviewed frameworks and were relevant to the experts' eyes were related to threats and vulnerabilities. The most common of these concepts included identifying and documenting the company's threats and vulnerabilities [39], [43], [44], [47], [48], [85], [88], [94], [95], [101], [103] and mitigating the company's threats and vulnerabilities [39], [47], [85], [88], [94], [95], [101], [104]. These concepts have been included under the domain titled "threat and vulnerability management" because similar concepts can be found under the same or similar titles in the reviewed frameworks [47], [85], [87], [88], [94].

Due to these common concepts and after iterating with the experts, the CR-CF includes the threat and vulnerability management domain with the following two main policies:

- Identify and document the company's threats and vulnerabilities.
- Mitigate the company's threats and vulnerabilities.

4.2.5 Incident Analysis

Several of the reviewed frameworks also referred to a group of concepts related to learning from the previously occurred incidents. These concepts often

included assessing the damages after an incident [37], [41], [43], [44], [87], [88], [103], determining the causes, objectives, points of entry and methods that enabled the incident [41], [43], [44], [85], [87], [88], [94], [103], and analyzing the responses and response selection process after an incident occurred [41], [43], [44]. These concepts are often mixed with the response to incidents under an incident management domain or similar [37], [41], [42], [85], [87], [88], [94], [103], [104]. However, the experts considered it important to separate the incident analysis from the incident response in order to stress a somewhat implicit concept in other frameworks related to learning from previously suffered incidents [41], [43], [44], [48], [87], [88], [104], and the management of the incidents was left for another domain. Thus, the title for this domain was chosen to be "Incident Analysis".

After grouping these concepts into the CR-CF and iterating with the experts, the incident analysis domain has the following policies:

- Assess and document the damages suffered after an incident.
- Analyze the suffered incidents to find as much information as possible: causes, methods, objectives, point of entry, etc.
- Evaluate the company's response and response selection to the incident.
- Identify lessons learned from the previous incidents and implement measures to improve future responses, response selections, and risk management.

4.2.6 Awareness and Training

Another recurrent theme in the reviewed frameworks that the experts considered important for a CR-CF was related with maintaining the personnel trained and aware of their role in the company's cyber resilience. This includes creating training and awareness plans [42], [47], [48], [104], making sure the company's employees had the adequate training for their roles in the cyber resilience strategy [37], [39], [41], [42], [47], [48], [87], [94], [95], [104], raising the company's employees' awareness [41]–[44], [47], [48], [87], [104], and training the personnel in technical skills [37], [39], [42], [47], [48], [87], [94], [102], [104]. These concepts have been grouped under the "awareness and training" domain, because the title is used in several of the reviewed frameworks [41], [42], [48], [85], [88], [104].

Using these concepts and the experts' opinion, the awareness and training domain's policies are:

- Define and document training and awareness plans.
- Evaluate the gaps in the personnel skills needed to perform their cyber resilience roles and include these gaps in the training plans.
- Train the personnel with technical skills.
- Raise the personnel's awareness through training programs.

4.2.7 Information Security

The protection of confidentiality, integrity and availability (CIA triad) of information was another group of concepts found in most of the reviewed cyber resilience frameworks. The protection of the CIA triad can be found either directly mentioned or through commonly used practices to protect them. After discussion with the experts and to maintain the same level of specificity across the CR-CF the practices will not be listed as individual actions, but rather as examples of the protection of one of the parts of the components of the CIA triad. Based on this, the common concepts that have been grouped are protecting the confidentiality through network segmentation, cryptographic techniques in databases and communications, and access control [39], [41], [47], [48], [85], [87], [88], [94], [95], [104]. Protecting the integrity through integrity checking mechanisms in data, hardware, software, and firmware [39], [41], [42], [47], [48], [87], [88], [95], [104]. Finally, protecting availability through back-ups, redundancy and maintaining adequate capacity [39], [41], [44], [47], [48], [87], [88], [95], [104]. The protection of the CIA triad is often called "information security" [87], and thus this is used as the title for the domain that groups these concepts.

- The final information security domain's policies were written as follows:
- Implement measures to protect confidentiality (e.g. access control measures, network segmentation, cryptographic techniques for data and communications, etc.)
- Implement integrity checking mechanisms for data, software, hardware and firmware.
- Ensure availability through backups, redundancy, and maintaining adequate capacity.

4.2.8 Detection Processes and Continuous Monitoring

The reviewed frameworks commonly referenced measures to monitor the company's assets and detect incidents. Monitoring the company's assets includes the use of controls/sensors, Intrusion Detection Systems (IDS), Network Intrusion Detection Systems (NIDS), etc. [37], [39], [41]–[44], [47], [48], [85], [87], [88], [94], [95], [104]. And detecting incidents requires defining detection processes that clearly state when to escalate anomalous activity into incidents and have a protocol for notifying the appropriate parties in case of detection to trigger the appropriate response [37], [41]–[43], [88], [94], [103], [104]. These concepts are often found in the reviewed frameworks as "continuous monitoring" or similar [37], [41], [48], [104], however, to emphasize the objective of the monitoring, this study uses "detection processes and continuous monitoring" as the title that encompasses this group of concepts. The "detection process" is inspired by [41] in which both "continuous monitoring" and "detection processes" are part of the "detect" function.

Based on the common concepts found in the reviewed frameworks and the experts' inputs, the policies for this domain were written as follows:

- Actively monitor the company's assets (e.g. by implementing controls/sensors, IDS, NIDS, etc.).
- Define a detection process that specifies when to escalate anomalies into incidents and notifies the appropriate parties according to the type of detected incident.

4.2.9 Business Continuity Management

Another commonly referenced group of concepts that the experts' evaluations considered relevant is related to planning for contingencies. This group of concepts included the definition of plans to maintain business operations despite adverse conditions [37], [41], [47], [48], [87], [88], [94], [95], [102]–[104], to determine actions and responsibilities in order to recover normal operations and define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) [37], [39], [41]–[44], [47], [48], [85], [87], [88], [94], [95], [103], [104], and to test these business continuity plans periodically to determine their effectiveness and adjust them accordingly [37], [41], [42], [47], [87], [88], [94], [95], [103], [104]. These concepts have been grouped under the domain

titled "Business Continuity Management" because "service continuity management" and "business continuity management" are commonly used titles to group similar concepts in the reviewed frameworks [37], [48], [87], [95], [104] and "business continuity" was considered the better option by the experts.

Considering these concepts and after iterating with the experts, the policies for this domain of the CR-CF were written as follows:

- Define and document plans to maintain the operations despite different scenarios of adverse situations.
- Define and document plans to respond to and recover from incidents that include recovery time objectives and recovery point objectives.
- Periodically test the business continuity plans to evaluate their adequacy and adjust them to achieve the best possible operations under adverse situations.

4.2.10 Information Sharing and Communication

Finally, the reviewed frameworks had a group of concepts related to collaboration and communication. The group of these concepts relevant for SMEs according to the experts include cooperating with external parties to receive and report useful information about cyber resilience issues and receive assistance for business continuity [37], [41], [43], [44], [47], [64], [88], [94], defining communication plans for emergency situations that include management of public relations, reparation of the reputation, and communication of the suffered incident to all the appropriate parties [37], [41], [47], [94], [102], and collaborating with the company's suppliers and third party partners to implement the appropriate measures to meet the company's cyber resilience needs [41], [47], [48], [64], [87], [94], [95], [102], [104]. This group was titled "information sharing and communications" because this title or a similar one are used by several of the reviewed frameworks to group similar concepts [37], [47], [64], [94] and it was considered the most appropriate by the experts.

Finally, the information sharing and communication domain affects all of the cyber resilience lifecycle. Sharing information can let the company be aware of newer threats, know how to detect them, how to resist them (withstand), how to recover from them and how to evolve afterwards [86].

SMEs can benefit most of all companies from collaboration with other, more experienced companies since it is an opportunity for the company to learn from them. In this sense, this domain can help SMEs learn more about cyber resilience implementation and take these lessons to implement other domains in this conceptual framework, thus reducing the necessary resources for the implementation.

Based on the above-mentioned concepts and the experts' input, the policies for this domain were written as follows:

- Define information sharing and cooperation agreements with external private and public entities to improve the company's cyber resilience capabilities.
- Define and document a communication plan for emergencies that takes into account the management of public relations, the reparation of the company's reputation after an event, and the communication of the suffered incident to the authorities and other important third parties.
- Establish collaborative relationships with the company's external stakeholders (e.g. suppliers) to implement policies that help each other's cyber resilience goals.

After describing the 10 domains and its policies' origin, Table 4.1 CR-CF and other frameworks influences presents a summary of the domains, policies and the references that include them. The contents of Table 4.1 CR-CF and other frameworks influences display:

- A "#" when the reference in the column refers to the policy in the corresponding row in the text of the document, but not directly as a policy or domain.
- An "x" when the reference contains at least one policy, control or question about the policy in the corresponding row.
- A "●" when the reference contains a domain centered around that policy.
- And an "!" when the policy in the corresponding row is the main focus of the reference in the column.

Table 4.1 CR-CF and other frameworks influences

		Reference to analyzed documents with indexes from Table 3.1																	
Domain	Policy	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Governance	Develop and communicate a cyber resilience strategy.			!			#	!		#	#	#		x	!	x		●	
	Comply with cyber resilience-related regulation.			x				●				x	●	x					
	Assign resources (funds, people, tools, etc.) to develop cyber resilience activities.	x			x													x	
Risk Management	Systematically identify and document the company's cyber risks.	!	!		x			!		x	x		x		!	x		x	
	Classify/prioritize the company's cyber risks.							!		x	x		x			x	x	x	
	Determine a risk tolerance threshold.				x					x	x		x		!	x			
	Mitigate the risks that exceed the risk tolerance threshold.	!	!		x			!	x	x	x		x	x	!	x		x	
Asset Management	Make an inventory that lists and classifies the company's assets and identifies the critical assets.				x			#	x	x	x		x			x	●	x	x
	Create and document a baseline configuration for the company's assets.								x	x	x		x			x	●	x	
	Create a policy to manage the changes in the assets' configurations.								x	x	x		x			x	x	x	
	Create a policy to periodically maintain the company's assets.				x			●	x	x	x		x				●	x	x
	Identify and document the internal and external dependencies of the company's assets.				x		x			x	●	x	●					●	
Threat and Vulnerability Management	Identify and document the company's threats and vulnerabilities.	!	!		x	x	x		x	x	x	x		x				x	
	Mitigate the company's threats and vulnerabilities.	!	!			x				x	x			x				x	
Incident Analysis	Assess and document the damages suffered after an incident.				x		x	#			x	x				x			x
	Analyze the suffered incidents to find as much information as possible: causes, methods, objectives, point of entry, etc.				x		x	#			x	x		x		x			
	Evaluate the company's response and response selection to the incident.						x					x				x			
	Identify lessons learned from the previous incidents and implement measures to improve future responses, response selections, and risk management.						x		x		x	x	x			x			
Awareness and Training	Define and document training and awareness plans.								x	x			x				●		
	Evaluate the gaps in the personnel skills needed to perform their cyber resilience roles and include these gaps in the training plans.		x			x		#	x	x			x			x	x	x	x
	Train the personnel with technical skills.			x		x		#	x	x			x				x	x	x
	Raise the personnel's awareness through their training programs.						x	#	x	x		x	x			x	x		
Information Security	Implement measures to protect confidentiality (e.g. access control measures, network segmentation, cryptographic techniques for data and communications, etc.)		x			x		●	x	●	x		x	●		x	x		
	Implement integrity checking mechanisms for data, software, hardware and firmware.		x			x		#	x	x	x		x			x		x	
	Ensure availability through backups, redundancy, and maintaining adequate capacity.		x			x		#	x	x	x	x	x			x			
Detection Processes and Continuous Monitoring	Actively monitor the company's assets (e.g. by implementing controls/sensors, IDS, NIDS, etc.)		x			x	x	x	x	x	x	x	●	x		x	●	x	x
	Define a detection process that specifies when to escalate anomalies into incidents and notifies the appropriate parties according to the type of detected incident.				x		x				x		x			x	x	x	x
Business Continuity Management	Define and document plans to maintain the operations despite different scenarios of adverse situations.		x	x	x			●	x	x	x		x		x	x		x	x
	Define and document plans to respond to and recover from incidents that include recovery time objectives and recovery point objectives.		x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Periodically test the business continuity plans to evaluate their adequacy and adjust them to achieve the best possible operations under adverse situations.		x		x			x		x	x		x		x	x	x	x	x
Information Sharing and Communication	Define information sharing and cooperation agreements with external private and public entities to improve the company's cyber resilience capabilities.						x			x	x	x			x	x		x	x
	Define and document a communication plan for emergencies that takes into account the management of public relations, the reparation of the company's reputation after an event, and the communication of the suffered incident to the authorities and other important third parties.			x			x			x			●			x		x	x
	Establish collaborative relationships with the company's external stakeholders (e.g. suppliers) to implement policies that help each other's cyber resilience goals.		x	x				●	x	x			x		x	x		x	

4.3 Implementation Order

Up to this point, the CR-CF identifies the essential domains and policies required to operationalize cyber resilience. However, having a list of required actions does not clarify how to prioritize these actions. Moreover, the experts considered that the policies' implementation order could influence their effectiveness as well. For instance, they argued that trying to implement information security measures without first classifying the assets could result in unnecessary investment in the protection of assets that are not critical to the company's process or business continuity and in a lack of protection to those important assets. This is also supported by the literature as exemplified in the relationship between implementing detection systems and the relationship with training [100]. In turn, an incident that affects an unprotected critical asset could represent high costs [22], [131], [132] and a company that has invested considerably in protecting other assets could lead to the assumption that "spending" in cyber resilience is not effective.

Thus, the experts were asked to develop an implementation order to be used as a guideline for SMEs to be able to prioritize cyber resilience operationalization. The following subsection shows a possible policy-level implementation order for the essential cyber resilience operationalization policies (the policies in the CR-CF). This implementation order can be used by the cyber resilience operationalization decision-maker in an SME to prioritize between the implementation of one policy or another.

4.3.1 Policy-Level Implementation Order

As defined in the CR-CF, there are 10 domains and 33 policies essential to the operationalization of cyber resilience. Amongst each domain, there are several policies.

By using the literature and the evaluation with the six experts, this study was able to define one implementation order that would be effective for cyber resilience operationalization using the policies inside the CR-CF. To arrange the policies in an implementation order and fit them into a diagram, the CR-CF was coded as shown in Table 4.2.

Table 4.2 Cyber Resilience Domains and Policies

Domain	Code	Policy
Governance	G1	Develop and communicate a cyber resilience strategy.
	G2	Comply with cyber resilience-related regulation.
	G3	Assign resources (funds, people, tools, etc.) to develop cyber resilience activities.
Risk Management	RM1	Systematically identify and document the company's cyber risks.
	RM2	Classify/prioritize the company's cyber risks.
	RM3	Determine a risk tolerance threshold.
	RM4	Mitigate the risks that exceed the risk tolerance threshold.
Asset Management	AM1	Make an inventory that lists and classifies the company's assets and identifies the critical assets.
	AM2	Create and document a baseline configuration for the company's assets.
	AM3	Create a policy to manage the changes in the assets' configurations.
	AM4	Create a policy to periodically maintain the company's assets.
	AM5	Identify and document the internal and external dependencies of the company's assets.
Threat and Vulnerability Management	TVM1	Identify and document the company's threats and vulnerabilities.
	TVM2	Mitigate the company's threats and vulnerabilities.
Incident Analysis	IA1	Assess and document the damages suffered after an incident.
	IA2	Analyze the suffered incidents to find as much information as possible: causes, methods, objectives, point of entry, etc.
	IA3	Evaluate the company's response and response selection to the incident.
	IA4	Identify lessons learned from the previous incidents and implement measures to improve future responses, response selections, and risk management.
Awareness and Training	AT1	Define and document training and awareness plans.
	AT2	Evaluate the gaps in the personnel skills needed to perform their cyber resilience roles and include these gaps in the training plans.
	AT3	Train the personnel with technical skills.
	AT4	Raise the personnel's awareness through their training programs.
Information Security	IS1	Implement measures to protect confidentiality (e.g. access control measures, network segmentation, cryptographic techniques for data and communications, etc.)
	IS2	Implement integrity checking mechanisms for data, software, hardware and firmware.
	IS3	Ensure availability through backups, redundancy, and maintaining adequate capacity.
Detection Processes and Continuous Monitoring	DPM1	Actively monitor the company's assets (e.g. by implementing controls/sensors, IDS, etc.)
	DPM2	Define a detection process that specifies when to escalate anomalies into incidents and notifies the appropriate parties according to the type of detected incident.
Business Continuity Management	BCM1	Define and document plans to maintain the operations despite different scenarios of adverse situations.

	BCM2	Define and document plans to respond to and recover from incidents that include recovery time objectives and recovery point objectives.
	BCM3	Periodically test the business continuity plans to evaluate their adequacy and adjust them to achieve the best possible operations under adverse situations.
Information Sharing and Communication	SHC1	Define information sharing and cooperation agreements with external private and public entities to improve the company's cyber resilience capabilities.
	SHC2	Define and document a communication plan for emergencies that takes into account the management of public relations, the reparation of the company's reputation after an event, and the communication of the suffered incident to the authorities and other important third parties.
	SHC3	Establish collaborative relationships with the company's external stakeholders (e.g. suppliers) to implement policies that help each other's cyber resilience goals.

Having said this, the experts divided the implementation order into eight sections and gave them names depending on the function they accomplish in the cyber resilience operationalization process (Figure 4.2, eight sections are color coded). Although cyber resilience has been divided into domains in the CR-CF, these grouping of policies is different because policies from the same domain should not necessarily be implemented at the same time, as it is explained in the following subsections. Moreover, as shown in Figure 4.2, there are two main sets of policies separated into two boxes: the transversal aiding policies which by themselves do not build cyber resilience but support the rest of the policies and improve their effectiveness; and the core cyber resilience building policies which are the policies that directly build cyber resilience and are ordered from left to right according to what the experts believe is an effective way to implement them.

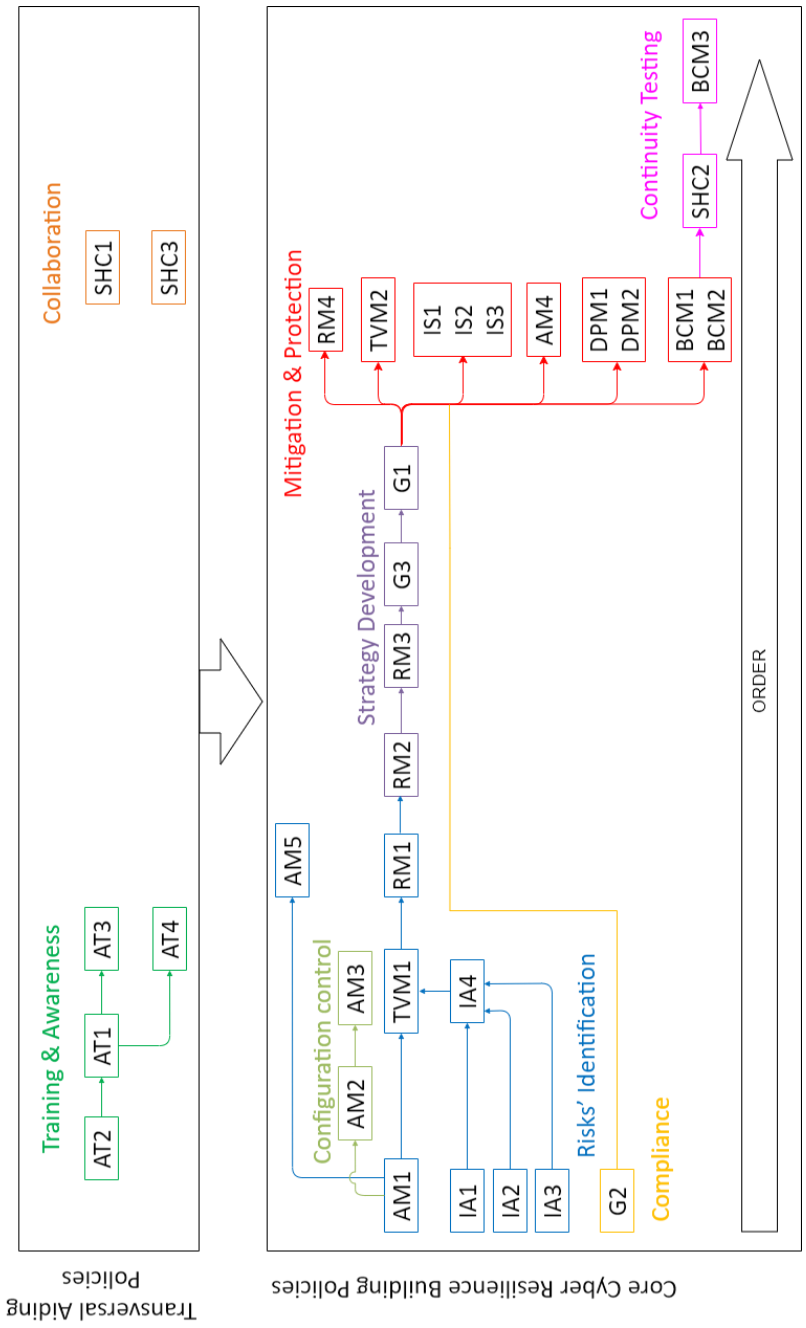

Figure 4.2. Cyber Resilience Policies' Implementation Order

A. Risk Identification

According to the experts and the literature, the first steps towards building cyber resilience are making the inventory or assets with their respective classification (AM1) in order to determine their possible threats and vulnerabilities (TVM1) [101]. Both, the experts and the literature, then agreed that in order to make an effective risk management evaluation and threat and vulnerability evaluation the company could be aided by the analysis of their previous incidents. In this sense, they suggested that the company assessed and documented the damages of the cyber incidents that they suffer (IA1), analyze the methods, causes, etc. for these incidents (IA2) and evaluate their responses to these incidents (IA3) in order to learn as much as possible from them (IA4), and help them identify threats and vulnerabilities (TVM1) [88], [101].

Once the technical threats and vulnerabilities have been identified, the experts and the literature suggest that the rest of the risks should be identified (RM1) [101]. In order to identify all the risks, the internal and external dependencies of the assets should be identified (AM5).

Thus, as described before, the Risk Identification group of policies are related to the Asset Management, Threat and Vulnerability Management, Risk Management and Incident Analysis domains in the CR-CF.

B. Compliance

According to the experts, before going through the risk identification and the strategy development sections of the implementation order, any implementation of the mitigation and protection section could be inefficient. Their rationale for this is that the company could over protect assets or over invest in security measures for vulnerabilities that are not critical, leaving the most critical risks exploitable and their most critical assets vulnerable. However, they argued that there is an exception to this since in some cases complying with regulation (G2) could make it necessary for the company to invest in some of these measures. Moreover, the literature also emphasizes the importance of complying with regulation as part of cyber resilience management and operationalization [51]. For these reasons, compliance (G2) can be done at the beginning of the cyber resilience operationalization as shown in Figure 4.2.

As described compliance would only be related to the CR-CF's Governance domain.

C. Strategy Development

After the risk identification process, the company should classify and prioritize their risks (RM2) and determine their risk tolerance threshold (RM3). Depending on this threshold and their current risks and priorities, the company should assign the resources they are willing to use for cyber resilience (G3). With these inputs, the company should decide which assets to protect and how by defining a cyber resilience strategy (G1). A similar approach is suggested in the literature where the cyber resilience strategy is based in the current threats [41], [51], [88], [101].

Thus, as described, the Strategy Development group of policies are related to the Governance and Risk Management domains in the CR-CF.

D. Mitigation and Protection

After defining a strategy, the company should have clear ideas on how to mitigate risks (RM4) and vulnerabilities (TVM2) through the maintenance of the assets (AM4); the implementation of the information security measures (IS1, IS2 and IS3); the implementation of continuous monitoring tools and a detection process (DPM1 and DPM2); and through the planning of how to respond and recover from incidents (BCM1 and BCM2). Similar ideas are also alluded in the literature [41], [51], [101].

As described the Mitigation and Protection policies are related to the Risk Management, Threat and Vulnerability Management, Asset Management, Information Security, Detection Processes and Continuous Monitoring, and Business Continuity Management domains in the CR-CF.

E. Continuity Testing

According to the experts, after implementing the mitigation and protection section of the implementation order, companies should include the way in which they will deal with third parties in case of an incident in their business continuity plans. This means that they should make communication plans for these cases (SHC2). Both, the business continuity plans, and the communication plans should be tested periodically to improve them iteratively (BCM3).

Therefore, the Continuity Testing group is related to the Business Continuity Management and the Information Sharing and Communication domains in the CR-CF.

F. Configuration Control

As shown in Figure 4.2, in parallel to the strategy development, and just after implementing section of the risk identification, companies could implement configuration control (colored light green). This section of the implementation order consists of creating a baseline configuration for all the assets (AM2) and later a configuration change policy (AM3) in order to keep traceability of the changes and in order to be able to reverse them in case they have unexpected consequences.

This section of the process is, according to the experts, not as much of a priority as following the strategy development and the mitigation and protection sections. However, it can be done in parallel and if companies have the resources to do it, they should.

Thus, the Configuration Control is related to the Asset Management domain in the CR-CF.

G. Training and Awareness

The experts agreed that training of the personnel played an important role in the cyber resilience building process. They agreed that in order to efficiently implement training policies the company should identify gaps in the skills needed to perform cyber resilience activities (AT2). With these gaps in mind, they should plan awareness and technical training plans for the personnel (AT1) [51], [104]. With these plans, they should impart both technical and awareness training to the personnel (AT3 and AT4).

Both the experts and the literature [41], [51], [104] suggest that training is needed to perform well in any of the other cyber resilience policies (technical and non-technical). Thus, they considered it a transversal section of the process that should be implemented in parallel to the implementation of every other cyber resilience policy.

Thus, as described, the Training and Awareness group is equivalent to the Awareness and Training domain in the CR-CF.

H. Collaboration

Finally, the experts stated that establishing cooperation agreements with both, private and public entities (SHC1) and the company's external stakeholders (SHC3), help the rest of the implementation order since it can aid the company in the implementation of those policies and the company can also share their knowledge with these external entities. However, unlike training and awareness, which could be crucial in order to implement other cyber resilience policies, the experts considered these information sharing and communication policies as an aid that should be used after implementing the policies inside the "core cyber resilience building policies" rectangle in Figure 4.2.

Therefore, as described, the Collaboration group of policies is related to the Information Sharing and Communication domain in the CR-CF.

4.4 Progression Model

After defining the essential policies and guidelines for prioritizing them, companies also require guidelines on how to implement policies and later improve them. This information can be represented through a progression model. Thus, this section will present the results obtained from applying the previously described methodology (Section 3.4) to develop the progression model. As described in that section, 11 semi-structured interviews with experts were made to develop the progression model. After the 11 experts were interviewed and the transcripts were analyzed, 10 progression types were obtained. Table 4.3 defines the progression types found during the analysis of the transcripts. These progression types were later used for the coding step as described in the methodology chapter (Section 3.4).

Table 4.3 Progression types for coding and their definitions

Category	Definition
Investment Increase	This code was assigned when the expert's progression description was related to an increase in the resources (mainly economic resources) dedicated to implementing/ operationalizing the policy.
Continuity	This code was assigned when the expert's progression description was based on the increase of frequency in which the policy's actions are performed in the company (i.e., it was done more and more frequently as the level increased).
Specificity	This code was assigned when the expert's progression describes an increase in level of detail in which the policy is done as the maturity of the company increases. (i.e., it started in a general way and became more detailed and specific as the level increased).
Expansion	This code was assigned when the expert's progression description included the expansion of the policy's action in the company (e.g., the action was performed in some sections of the company and it started being done in more sections as the level increased).
Formalization	This code was assigned when the expert's progression description referred to the documentation or systematization of the actions (i.e., when the policy's actions started being intuitive or informal and where standardized and documented as the level increased).
Independence	This code was assigned when the expert's progression description mentioned the decrease of dependency of the company from the help of cybersecurity providers or external entities to perform the tasks related to the policy.
Optimization	This code was assigned when the expert's progression description was based on the measurement and improvement of Key Performance Indicators (KPIs) to optimize the performance of the policy's actions.
Proactivity	This code was assigned when the expert's progression description represented a change of attitude from the company towards the policy's actions (e.g., from complying to pursuing it for their own perceived benefit). The mention of continuous improvement in actions that could not be quantified was coded under this category as well.
No progression	This code was assigned when the expert considered that the policy was implemented and had no further progression, or when the starting maturity was considered to be at level 5.
Technology	This code was assigned when the expert's progression description was related to an increase in technological solutions or required more advanced technologies for the progression of the policy.

Following, the results of the progression model are presented in different subsections corresponding to each of the cyber resilience domains. In these subsections the results will be presented, but the tables with data used to get these results are presented in Appendix D.

The following sections show the example natural progressions obtained from the consensuses on the initial maturity states and progression types. Although during the interviews no name or description was given for the

maturity states (simply named as a scale of 1-5), a possible naming for these drawn as a conclusion from the examples in the following sections is shown in Table 4.4.

Table 4.4 Possible naming for the maturity states

Maturity Level	Possible Name	Description
0	None	The company does not have anything in most cyber resilience policies.
1	Incipient	The company has started the basic measures and commonly known cybersecurity actions.
2	Basic	The company has implemented most of the basic cybersecurity actions.
3	Formalizing	The company has started to document and define systematic processes to maintain and improve their cyber resilience.
4	Advanced	The company has systematic processes to implement standardized, periodic actions to maintain and improve their cyber resilience.
5	Optimized	The company has the most advanced actions implemented and they have optimized their implementation with continuous improvement.

In each of the following subsections, the initial maturity level, the progression types for each policy in the corresponding domain, and a table with the example progression is shown.

4.4.1 Governance

As a result of the described methodology (Section 3.4) consensus was found on the starting maturity levels for the first two policies. This consensus was determined to be level 2 for G1, level 1 for G2. Although G3 had no consensus on where the policy should start to be implemented the mode starting maturity level was used to construct an example progression.

Similarly, there was a consensus on the progression types for G1 and G2, but no consensus on the progression type of G3. However, to present an example progression the mode was used[1]. Therefore, the determined progression types were proactivity for G1, expansion for G2 and optimization for G3. With the

[1] The mode criteria was used to determine the non-consensuses found in other policies as well.

starting maturity levels for each policy, their progression types and the experts' example progressions a progression model was constructed. This progression model for the governance policies is shown in Table 4.5.

4.4.2 Risk Management

In the case of the risk management domain, there was consensus on the starting maturity level for all of its policies in maturity level 2. Their progression types were mostly considered by the experts to be formalization, except for RM4, which was considered to have an expansion progression type. Using this information and the experts' example progressions, the progression model for risk management policies shown in Table 4.6 was constructed.

4.4.3 Asset Management

For the asset management domain, this study found that the starting maturity level for AM1 was level 1, for AM2 was level 3 and for AM3, AM4 and AM5 it was level 2. Furthermore, their progression types were considered to be: specificity for AM1, a combination of formalization and technology for AM2 and AM3, proactivity for AM4, and a combination of formalization and proactivity for AM5. The starting maturity levels, the progression types and the example progressions from the experts were used to construct the progression model for asset management policies shown in Table 4.7.

4.4.4 Threat and Vulnerability Management

In the threat and vulnerability management policies, the consensus on their starting maturity levels were level 2 for TVM1 and level 3 for TVM2. Moreover, their progression types were determined to be formalization and optimization respectively. With this information the progression model shown in Table 4.8 was constructed.

Table 4.5 Governance policies' progression model

Policy	1	2	3	4	5
G1	N/A	There is a cyber resilience strategy that centers on protecting the systems according to their risks (implement traditional cybersecurity).	The cyber resilience strategy defines resilience requirements based on the risks of the company's assets. The company tries to comply with these resilience requirements to the best of their abilities. This includes having response plans in case of incidents that could harm the compliance with these requirements.	The company's strategy is detailed and tries to go in depth on how to make the systems and processes as resilient as possible with specific plans on how to recover in case the protection methods fail.	The strategy is continuously improved upon, trying to implement lessons learned from the company's previous iterations of the strategy and previous successes or mistakes.
G2	The company has identified the cyber resilience or cybersecurity related laws and regulations that directly concern their activity.	The company does its best to comply with the most directly related cyber resilience/cybersecurity laws and regulations.	The company tries to comply with the laws and regulations that have been identified by internally auditing which are being complied with and which are still in progress.	The company starts exploring laws and regulations that can indirectly concern their activity and sees added value in complying with these laws as a way to improve their cyber resilience.	The company continuously complies with more demanding regulations driven by their own cyber resilience implementation and not simply with the intention of complying.
G3	N/A	N/A	Specific, documented budgets and resources are assigned for the fulfillment of the cyber resilience strategy.	The investments in cyber resilience are controlled through KPIs that the company has elected to try to optimize their allocation of resources.	Resources are flexibly moved in order to maximize the benefits of the resources that have been assigned and optimize the values of the company's KPIs.

Table 4.6 Risk management policies' progression model

Policy	1	2	3	4	5
RM1	N/A	Risks are determined intuitively and according to the experience of the personnel.	A list of risks associated to the company's assets has been put together based on some research that tries to determine all the risks associated to the assets.	There is a systematic procedure used to identify all the risks associated to the company's assets. This procedure includes research, vulnerability management, etc. Risks are formally quantified according to their impact and probability.	The systematic procedure used to identify risks is repeated periodically to update the risks in the company. As much sources of information are used to identify these risks, including information from maintenance such as mean time before failure and mean time to recovery (used to calculate probability of downtime).
RM2	N/A	Identified risks are prioritized intuitively, according to the experience of the personnel and based on urgency towards the development of the company's activity.	Risks are classified and prioritized based on research of the impact they may have in the company's activity. This classification and prioritization are now documented.	Risks are calculated based on their impact and probability. The numerical risk values are considered when prioritizing risks. There is rigorous documentation of the risk associated to all the company's assets.	The systematic and formal risk classification and prioritization is updated periodically to have a realistic measure of the company's risk.
RM3	N/A	The risk tolerance threshold is put arbitrarily, mostly based on the abilities of the company's personnel to address the identified risks.	Risk tolerance is based on the possible impact of the risks.	The risk tolerance threshold is documented as a value of risk (impact x probability).	The risk tolerance threshold is continuously updated to more demanding values as the company's cyber resilience measures minimize risk.
RM4	N/A	The company mitigates some of the risks that have been identified and that affect the most important assets.	The company mitigates all the risks that affect important assets and some other risks that they can address.	The company mitigates most of the risks that exceed the risk tolerance threshold.	The company systematically mitigates all the risks (including newly discovered ones) that surpass each update of the risk tolerance threshold.

Table 4.7 Asset management policies' progression model

Policy	1	2	3	4	5
AM1	There is a list of the company's assets.	The company's inventory includes more information about the assets such as model, manufacturer, etc.	The company's inventory also includes the physical and logical location of the assets.	The inventory of the company's assets includes specific information about components in assets in which this may apply.	The company's inventory is highly specific with as much information of the assets as possible (e.g., components, make, value, location, risk value, etc.)
AM2	N/A	N/A	An undocumented base configuration is used to set up new systems in the company.	There is a documented base configuration for the company's assets. A Configuration management database (CMDB) is used to control document the base configurations	The base configuration of the company's assets is standardized and used in all of the systems. The CMDB is automatically updated as new assets are introduced or configurations are changed.
AM3	N/A	The company controls basic changes that have been made due to corrective maintenance issues.	The company's personnel starts to control the changes needed for the informal base configuration.	The company documents and has traceability of the changes made to the base configuration of the systems through a CMDB,	The traceability of changes made to any system in the system is registered in the CMDB as soon as possible after a change to a configuration has been made and through a standard, documented procedure.
AM4	N/A	The company does corrective maintenance to its assets.	The company occasionally updates the systems.	The company periodically does preventive maintenance and tries to keep the systems up to date.	The company has a system of predictive maintenance based on previous data of mean time before failure and mean time to repair.
AM5	N/A	The main dependencies are identified because of the knowledge of the company's personnel.	There is a documented list of the identified dependencies between systems.	The dependencies are systematically identified for all of the company's assets and documented in the dependency list.	The company does its best to identify all the internal and external dependencies from all of its assets and keep the dependency list updated in order to ease the contingency/business continuity planning.

Table 4.8 Threat and vulnerability management policies' progression model

Policy	1	2	3	4	5
TVM1	N/A	Threats and vulnerabilities are identified intuitively and according to the experience of the personnel.	There is a list of threats and vulnerabilities associated to the company's assets that has been put together based on some research in vulnerability repositories.	There is a systematic procedure (i.e., pen testing) used to identify all the threats and vulnerabilities associated to the company's assets.	The systematic procedure used to identify threats and vulnerabilities is repeated periodically to update the risks in the company.
TVM2	N/A	N/A	Threats and vulnerabilities that are perceived as priorities are mitigated as soon as possible and other vulnerabilities are mitigated in arbitrary order.	Threats and vulnerabilities are quantified as risks and they are mitigated if they exceed the risk tolerance threshold.	All threats and vulnerabilities are mitigated (including newly discovered ones) when they exceed the latest update of the risk tolerance threshold.

4.4.5 Incident Analysis

In the incident analysis domain, the starting maturity level for its policies was determined to be level 2 for IA1, level 3 for IA2 and IA4, and level 5 for IA3. Regarding their progression types, the analysis revealed that formalization was the main progression type for IA1 and IA4, specificity was the main progression for IA2, and there was no progression for IA3 since it already had to start at the highest possible maturity level. Using these results, the progression model presented in Table 4.9 was developed.

4.4.6 Awareness and Training

In the case of the awareness and training policies, their starting maturity levels were determined to be level 3 for AT1 and AT3, level 4 for AT2, and level 1 for AT4. The progression types for these policies were also analyzed and the results were: specificity for AT1 and AT3, continuity for AT2, and formalization for AT4. Using the experts' progression examples and these results, the progression model for each awareness and training policy shown in Table 4.10 was constructed.

4.4.7 Information Security

For the information security policies, the starting maturity was considered by the experts to be at level 1 for the three policies. There was also a clear consensus that in all of the three policies, the progression type was mainly technological. Using this information and the experts' inputs, the progression model for each policy shown in Table 4.11 was constructed.

Table 4.9 Incident analysis policies' progression model

Policy	1	2	3	4	5
IA1	N/A	The company informally evaluates their losses after an incident and the systems that need repairing or replacing.	The company evaluates their losses and documents them.	The company has a documented procedure to evaluate the damages caused by an incident.	The company has a documented and systematic (using the dependencies) procedure to evaluate all the systems after an incident in order to detect all of the incident's consequences.
IA2	N/A	N/A	The company does general forensics to determine the way in which the incident happened.	The company tries to identify the methods and entry points after an incident.	The company does a full forensics evaluation in which causes, methods, and entry points are fully discovered.
IA3	N/A	N/A	N/A	N/A	There is a systematic procedure to evaluate the company's response and response selection after every incident in order to improve decision-making in future incidents.
IA4	N/A	N/A	The company learns from the information obtained from the incident analysis and thus from the occurrence of every incident.	The company uses a documented procedure to identify lessons from previous incidents based on the way their forensics analysis and damage analysis is made.	The company systematically implements the lessons learned from incidents and documents them for future reference.

Table 4.10 Awareness and training policies' progression model

Policy	1	2	3	4	5
AT1	N/A	N/A	There is a general cyber resilience training plan for all the employees in the company.	There are plans defined according to different profiles of the employees.	Each employee has training plans according to their needs and gaps in abilities.
AT2	N/A	N/A	N/A	The company evaluates the gaps in the personnel abilities to perform their cyber resilience tasks in order to define the training plans.	The company periodically evaluates the gaps in the personnel's knowledge and abilities in order to keep the plans updated.
AT3	N/A	N/A	The technical personnel receives general technical training.	All the personnel receives technical training needed according to their profile and general tasks performed by employees from that profile.	All the personnel receives technical training according to their specific (personal) needs and gaps in their abilities.
AT4	N/A	There are undocumented and/or unfollowed cyber resilience rules for everyone related to their awareness.	There are occasional awareness communications for basic cyber resilience measures in which all the employees can participate.	There are periodical (with a defined period), documented and planned awareness training sessions or communications in the company.	The company systematically and periodically does awareness training courses or communications for the employees such as spam exercises, training sessions, etc.

Table 4.11 Information security policies' progression model

Policy	1	2	3	4	5
IS1	The company has basic measures to protect confidentiality (e.g., access control for computers and systems)	The company has implemented permission levels into the network and systems, and the access control is both physical and digital.	The company has a rigorous control of who can access the data and registers when someone has accessed it, from where, what that user has done, etc.	The company uses cryptographic techniques to give another protection level to the company's most important data.	Both stored data and communications are automatically encrypted to ensure confidentiality.
IS2	Integrity measures are the same as confidentiality measures for the company at the moment.	N/A	N/A	Redundant data automatically double checks the integrity of the information after each modification of a register to ensure that it has not been tampered with.	The company has implemented integrity checking mechanisms such as checksums, digital certificates, block chain databases, etc. to ensure that the most important data and communications is not tampered with.
IS3	The company has basic measures to ensure availability, but mainly a backup to restore availability in case of an incident.	Manual backups are made periodically of the information in all of the systems of the company and stored in hard drives disconnected from the network.	The most important data in the company is automatically backed up into several redundant copies outside the network.	There are redundancies for the most important systems in order to ensure the availability of these systems.	The company has the most advanced availability measures such as redundant high availability data processing centers with hot swapping techniques or other multiple copy methods that ensure that the data is always available.

4.4.8 Detection Processes and Continuous Monitoring

In the detection processes and continuous monitoring domain, the starting maturity levels for DPM1 and DPM2 were level 2 and level 3 respectively. Their progression types were determined to be expansion and technology for DPM1 and formalization for DPM2. Using these results, the progression model shown in Table 4.12 was constructed.

4.4.9 Business Continuity Management

In the case of business continuity management, the starting maturity for BCM1 and BCM2 the starting maturity level was determined to be level 3 and for BCM3 the consensus was on level 4. The main progression types for these policies were a combination of expansion and formalization in the case of BCM1 and BCM2, and continuity for BCM3. Using these starting maturity levels, the progression types and the example progressions given by the experts the progression model shown in Table 4.13 was developed.

4.4.10 Information Sharing and Communication

Finally, for the information sharing and communication domain, the starting maturity for its three policies was determined to be level 3. In this case, the progression types were a combination of formalization and proactivity for SHC1, specificity for SHC2, and formalization for SHC3. Using these results, the progressions shown in Table 4.14 were developed.

Table 4.12 Detection processes and continuous monitoring policies' progression model

Policy	1	2	3	4	5
DPM1	N/A	The company monitors some indicators (e.g., availability, workload, etc.) from the most important assets.	The company starts to monitor more indicators for the most important assets and starts to expand the number of assets monitored.	The company monitors most of its assets by monitoring several indicators from them. There is an alarm system that automatically detects anomalous behaviors.	The company has a complete picture of the company's operations from the monitorization of several indicators in all of the company's assets and an automatic alarm system when there is anomalous behavior.
DPM2	N/A	N/A	There is a basic, undocumented plan to call the corresponding parties when there is an incident (e.g., call IT).	There is a documented plan with clear instructions on what to do when there is an incident in the company.	There is a documented plan with clear instructions on what to do, how to communicate and to whom when there is an incident in the company.

Table 4.13 Business continuity management policies' progression model

Policy	1	2	3	4	5
BCM1	N/A	N/A	The company's personnel has in mind what to do in order to maintain operations of certain assets in case of certain incidents.	The company documents plans in order to protect the main assets in case of incidents.	There is a documented plan for the company's assets maintenance of operations in case of any type of incident. Plans to withstand maintenance failures are also considered and these failures are measured with the mean time before failure.
BCM2	N/A	N/A	The company's personnel has in mind what to do in order recover from certain types of incidents.	The company documents plans in order recover operations in case of the major types of incidents.	There is a documented plan for the company's recovery of operations in case of any type of incident. Plans to recover from maintenance failures are also taken into account and consider the mean time to repair.
BCM3	N/A	N/A	N/A	Business continuity plans are tested in order to determine their effectivity in the situations they are meant to be used.	Business continuity plans are tested periodically in order to improve them and check that they are still useful despite small changes that may have happened in the company during the assigned period.

Table 4.14 Information sharing and communication policies' progression model

Policy	1	2	3	4	5
SHC1	N/A	N/A	Some informal relationships with other entities are established mainly because of personal contacts from the personnel.	There are documented, formal and well-defined relationships between the company and some external entities to share information about cyber resilience.	The company actively seeks to establish more formal information sharing and cooperation relationships with external entities.
SHC2	N/A	N/A	There is a general resilience communication plan. In case any incident happens, this plan is activated.	The emergency communication plan differs in some cases depending on the type of incident that is suffered.	There are emergency communication plans defined that correspond to the possible incidents that the company may suffer (i.e., to the risks and response plans).
SHC3	N/A	N/A	Some informal relationships with the company's providers are established mainly because of personal contacts from the personnel.	There are documented, formal and well-defined relationships between the company and some external stakeholders to cooperate and follow certain guidelines about cyber resilience.	The company actively seeks to establish more formal cooperation relationships with external stakeholders. These relationships seek to secure the supply chain as much as possible.

4.5 Cyber Resilience Self-Assessment Tool (CR-SAT)

With the results shown up to this point in this chapter, the CR-CF could work as a checklist of domains and policies required for the operationalization of cyber resilience. On the other hand, SMEs can use the progression model states' descriptions to self-assess each cyber resilience policy by choosing the description that best fits their current situation.

Thus, in this section, the aforementioned results where unified into a tool that could aid companies in this process of self-assessing. To achieve this, the documents in the literature that contained assessment tools (such as [37], [47], [88], [94]) were studied and compared. However, as shown in Appendix A, although certain cyber resilience aiding documents contain assessment tools, none of them aid in the prioritization after the initial evaluation. Thus, the progression model's 33 policies were transformed into a questionnaire where each policy was a statement in which the user had to select a level of implementation and the policy's progression over time was used as the scale to choose from. This would let companies later choose actions to improve each policy from posterior states' descriptions.

To this end, for each policy, the first option in the scale was set to not having implemented the policy, while the other options were directly referencing the progression over time for that policy. An example of how the progressions were adapted to become scales is shown in Table 4.15.

Table 4.15 Example of the adaptation from the progression model into a scale for the questionnaire.

	Policy:	**G2. Comply with cyber resilience related regulation.**			
Maturity Level	-	-	Scale	0	The company is not aware of any cyber resilience related laws or regulations that apply to them.
	1	The company has identified the cyber resilience or cybersecurity related laws and regulations that directly concern their activity.		1	The company has identified the cyber resilience related laws and regulations that directly concern their activity.
	2	The company does its best to comply with the most directly related cyber resilience/cybersecurity laws and regulations.		2	The company does its best to comply with the most directly related cyber resilience laws and regulations.
	3	The company tries to comply with the laws and regulations that have been identified by internally auditing which are being complied with and which are still in progress.		3	The company tries to comply with the laws and regulations that have been identified by internally auditing which are being complied with and which are still in progress.
	4	The company starts exploring laws and regulations that can indirectly concern their activity and sees added value in complying with these laws as a way to improve their cyber resilience.		4	The company starts exploring laws and regulations that can indirectly concern their activity and sees added value in complying with these laws as a way to improve their cyber resilience.
	5	The company continuously complies with more demanding regulations driven by their own cyber resilience implementation and not simply with the intention of complying.		5	The company continuously complies with more demanding regulations driven by their own cyber resilience implementation and not for simple compliance.

Once this questionnaire was finished, the development process of a web-based prototype started. In this prototype, the following requirements were considered:

1. The tool should consist of 33 policies with their corresponding scales from which the user can choose one of the options as a current maturity state.
2. The user should be able to self-assess as many times as needed.
3. The user should be able to see the results at domain level and at policy level of the finished self-assessments.
4. The user should be able to use the tool in their preferred language to avoid misinterpretations. (For the purposes of this study, the prototype includes two languages, English and Spanish).
5. The tool should be flexible to future changes.

The technology stack used to develop the application used primarily JavaScript. In this sense, Node.js LTS 14.15.5 was used as the runtime environment to support the back-end of the application. To handle HTTP requests, the Express.js library (v. 4.17.1) was used and connected to a PostgreSQL (v. 13) database. To handle front-end templates, the Pug.js (v. 3.0) library was used in combination to Bootstrap 4.0 for styling.

Having the technology stack, the underlying research and the previously mentioned requirements, the prototype for the CR-SAT was developed. The sitemap for the prototype is shown in Figure 4.3.

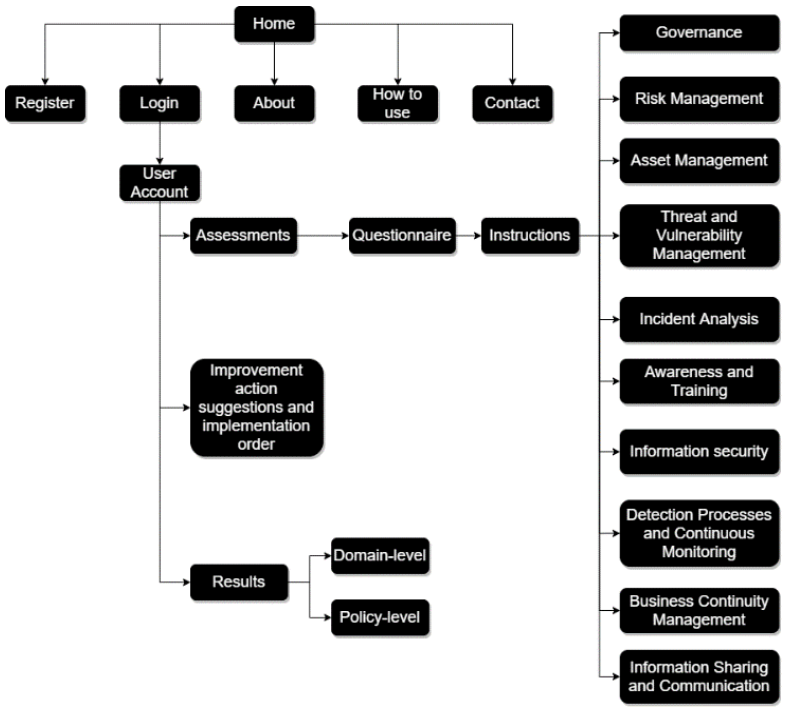

Figure 4.3 CR-SAT sitemap

In this prototype, the users could start as many assessments as they needed. They were also presented with a set of instructions that included the definitions of the domains (or categories) they were going to be evaluated in and an explanation of how to fulfill the questionnaire.

When the users start the self-assessment, they would be presented with the questions (which correspond to the policies in the progression model) and their scales (which correspond to the progression in the progression model). Each question has a designated space for the user to include evidences of their response selection, and a comments section that in certain policies will help clarify the statement in question or the meaning of possibly unfamiliar terms. An example of the interface for one question in the questionnaire is shown in Figure 4.4.

Figure 4.4 Questionnaire interface

Once the users finish the self-assessment, they can see the results report through different radar charts to aid in the comparison of the different states they achieved in different assessments.

Figure 4.5 shows an example of the results report shown to the users once they finish one or more assessments. As shown in the figure, the user can choose which assessments to graph in the report to be able to easily compare them. Once the user has selected one or more of their assessments to see their results' report they can see a domain-level radar graph in which they can see the average maturity they have in each domain. As shown in the interface, the user also has the option to see a graph for each domain in which they can see their maturity level in each policy of that domain. This visual overview can help companies identify their strengths and weaknesses at a domain level and once they decide which domain they would like to improve, they can visually identify the policies that require the most improvement.

Figure 4.5 Results dashboard

The target user of this tool is the decision maker in charge of cyber resilience operationalization. Depending on the company this decision maker could be the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), the Chief Executive Officer (CEO) or a member of the IT department. In some cases, this responsibility might be divided into several people in which case this group of decision-makers would ideally use the tool together.

Using the CR-SAT the decision-makers can also set objectives by filling an assessment with their wanted maturity states rather than their current state. This would help them have an overview of the differences between the current state and the objectives in the same radar graph.

Due to the nature of the tool, it can be used several times by the same company in order to check how the company is improving over time, check whether the actions are working as expected, and reset the goals after each assessment. The self-assessment, especially if it is done repeatedly over time can help the company gain awareness of their current situation and gain experience by trying to improve that situation. Moreover, the tool can be used for strategic planning since concrete actions for improving the company's current cyber resilience operationalization can be obtained from the descriptions of the objective states for each policy.

4.6 Cyber Resilience Cyber Range (CR)^2

As an additional aid for decision makers to be able to understand the effects of implementing cyber resilience policies, this research proposes the use of simulation models as awareness training tools. Since cyber ranges are defined as virtual environments in which a trainee can embark on hands-on activities and through them gain practical knowledge in cyber security [133] a set of simulation models with an interface serving as a training tool could be considered a cyber range. Thus, in this section, the development of simulation models as described in Section 3.5 of this document are explained. Moreover, this section describes how these models can be used as a cyber range for training and increasing the decision-makers' awareness on the importance of their decisions of investment and prioritization. In this sense, the end-user of the cyber range would be the

same end-user than the one for the CR-SAT: the person or group of people in charge of cyber resilience operationalization decision-making.

To develop SD models as described in the methodology chapter, several interrelationships between cyber resilience policies were identified from the literature and from the expert interviews. The interrelationships between the policies led to the development of reference modes or behaviors over time (BoT) that could be modelled and therefore several models showing these behaviors or reference modes and interrelationships were developed. These models were translated into the Insightmaker modelling and simulation engine and an interface was developed for decision makers to be able to experiment with them. The models with interfaces can be used as serious games or cyber ranges to raise awareness amongst SME decision makers in the field of cyber resilience.

To instantiate these results, one model will be explained with its behaviors and the lessons that a decision maker could learn by using it in the following subsections. This model was chosen for being the most general model including 5 different domains as possible investments.

4.6.1 CR Model

The model selected to exemplify the cyber range involves five input variables, which represent investment in five possible cyber resilience domains from the CR-CF. These five domains are: detection processes and continuous monitoring, information security, training and awareness, vulnerability management, and information sharing. Among each of these domains the model represent the investment in one representative policy. For instances, investing in detection processes and continuous monitoring in this case is simplified to be the policy of monitoring assets by installing continuous monitoring systems.

Based on the behaviors obtained from the literature and the experts, a Causal Loop Diagram (CLD) explaining the interrelationships between these five domains was developed and is shown in Figure 4.6.This CLD mainly shows how investments in cyber resilience policies can reduce the impact of cyber incidents in a company. In this particular case, impact also represents resources that are spent in ineffectively used time such as the one used to react to false alerts.

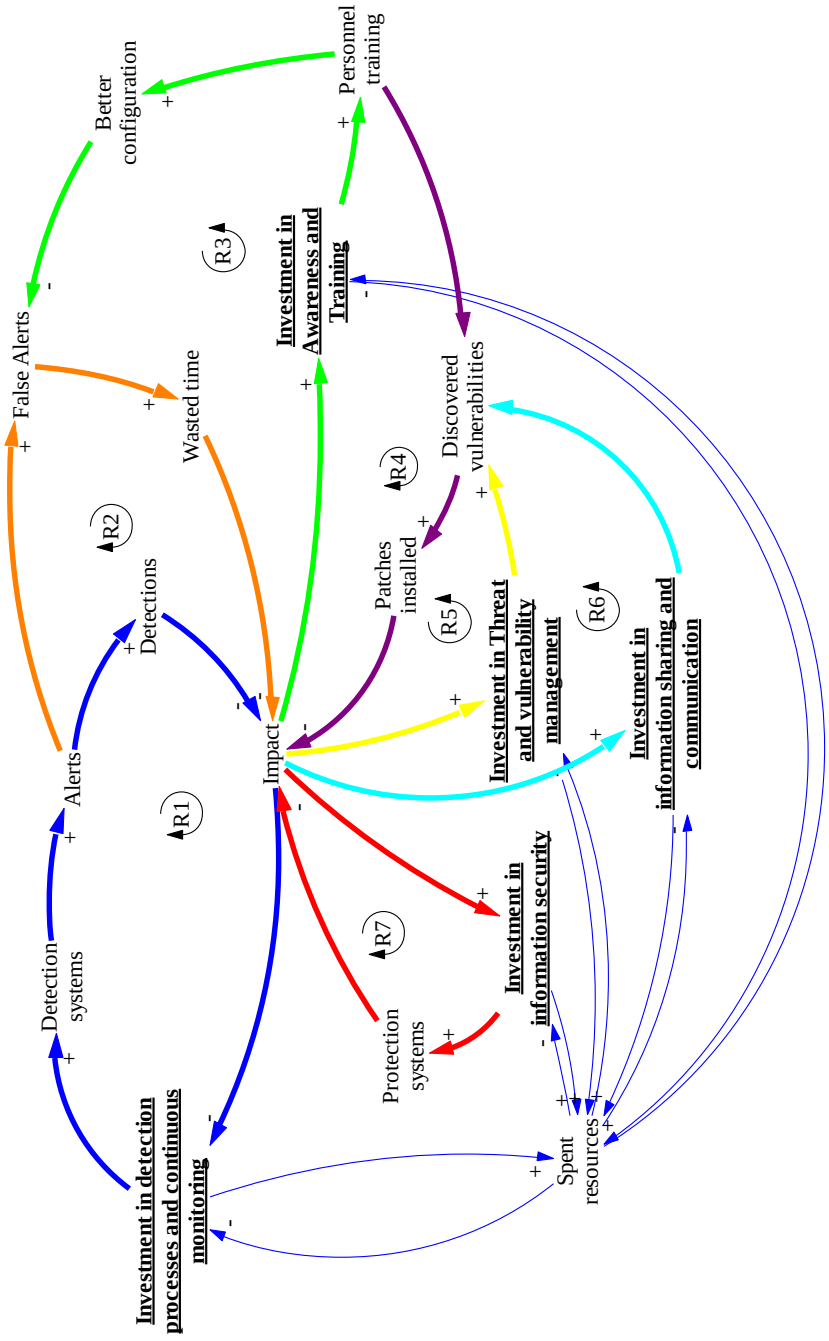

Figure 4.6 Causal Loop diagram

In the CLD, arrows represent causal relationships between variables, and the (+) or (-) signs represent whether the relationship is directly proportional (+) or inversely proportional (-). These causal relationships form causal loops that can either represent reinforcing behaviors (exponential or decaying behaviors) or balancing behaviors (limiting behaviors).

As marked in Figure 4.6, seven causal loops represent the effects of the investments decision makers can make and the interactions between these investments and the other domains. The marked causal loops are mostly reinforcing loops. These are not the only behaviors the model represents since there are several balancing loops that represent the limitation of resources. The easiest to notice out of these are the loops that form between the five possible investments and the spent resources. The more the decision makers invest in a policy, the less they can invest later. However, over 20 other loops can be found showing that the more the decision makers invest in one policy, the less they can spend in others. This can be understood as a "tragedy of the commons" system dynamics archetype [134] and it is a simple representation of a balancing behavior that most people are familiar with and that is important to acknowledge when making decisions about investments in any area.

The seven causal loops that represent the effects of decision makers' investments and their interactions are highlighted in different colors and have been numbered for reference in Figure 4.6. These causal loops can be explained as follows:

R1: Investment in detection processes and continuous monitoring allows the company to buy more detection systems. The more detection systems a company has the more alerts they generate. These alerts lead to detections and detecting incidents in time reduces their impact. Since there is less impact after investing in this domain, the decision maker will likely invest in this domain again, thus the last causal relationship being inversely proportional (less impact, more investment in detection).

B1: This loop balances the investment in detection processes and continuous monitoring. Following the loop shows that half of it is shared with loop R1. This loop shows that the more investment in detection, the more detection systems. The more detection systems, more alerts will be issued by these systems. The

more alerts there are, the more false alerts there will be. More false alerts will represent more wasted time spent checking these alerts and their cause. More wasted time will increase the impact because this time costs resources to the company. More impact will represent less investment in detection.

R2: This loop represents how awareness and training can mitigate the effects of B1. R2, R1 and B1 together represent a behavior well known to the cybersecurity literature [100]. As shown in R2, investment in training will represent better trained personnel. Having better trained personnel can help better configure the detection systems, reducing the false alerts. Reducing the false alerts reduces the time wasted and this reduces the impact. Since investing in training reduces the impact, the less impact the more investment in training.

R3: This loop is another direct effect of awareness and training. In this case it represents the relationship between training and vulnerability discovery. The more investment in training, the more trained the company's personnel will be. The more trained the personnel the better they will be to identify vulnerabilities. The more discovered vulnerabilities the more patched vulnerabilities there will be. As there are more patched vulnerabilities it is less likely to have a cyber incident and thus the less impact. The less impact there is the more investment in training because it worked.

R4: This loop represents the direct effect of investing in threat and vulnerability management. In this case, investment in vulnerability management leads to more discovered vulnerabilities. More discovered vulnerabilities will mean that more systems are patched. Patched systems are less likely to be exploited, and therefore there will be less impact from cyber incidents. Less impact will lead the decision maker to invest more in vulnerability management because it worked.

R5: This loop represents the effects of investing in information sharing and communication. This loop is a simplification that assumes that the only direct effect of information sharing has to do with discovering vulnerabilities. Having said this, in the model R5 is also related to R4 because it assumes that the information received from third parties is exclusively about vulnerabilities. This means that the more investment on information sharing, the more discovered vulnerabilities. The more discovered vulnerabilities, the more patches installed.

More installed patches reduce the likelihood of having cyber incidents, thus reducing the impact. Less impact will encourage the decision maker to invest more in information sharing.

R6: This final loop represents the effects of investing in information security. In this sense, the more investment in information security the more protection systems the company will have. The more protection systems, the less likely it is to have a cyber incident and therefore the less impact there is. Less impact will encourage the decision maker to invest more in information security because positive effects will encourage them to repeat the same strategies.

Using these theoretical behaviors found during the interviews and/or in the literature, different BoT graphs were obtained. One example of these BoT graphs can be explained as follows:

The scenario: this BoT represents a situation in which suddenly the company's decision makers start to invest 100% of their resources in detection processes and continuous monitoring (one of the five possible investments described before) with the intention to detect all the possible threats in time. In this figure, at the beginning, all policies start at 20% investment (the starting point defined for the model) and due to a decision to try to detect every possible threat at the fifth month, the investment in detection increases to 100%, while all others (training and awareness, threat and vulnerability management, information security, and information sharing and communication) decrease to 0%.

Because of this decision, the number of detections increases until it reaches a saturation due to not having more threats that are detectable in their current knowledge (because they are not investing in discovering more). Some other reasons for this saturation is the lack of discovered vulnerabilities in order to detect threats related to those and a lack of training and information sharing to be able to solve and manage the fewer discovered vulnerabilities that also causes this limitation. The saturation of the detections is shown in Figure 4.7 (orange line).

Conversely, as an unintended consequence the number of false alerts increases along with the increase in detections as shown in Figure 4.7 (red line). The main reason behind this unintended consequence would be the lack of

investment in training which according to both, the literature and the experts, leads to poor handling of the alerts in detection systems [100].

Moreover, as new detection systems are installed in the company, new vulnerabilities arise in the current systems and fewer systems are protected, the percentage of patched systems decreases, as shown in Figure 4.7 (blue line). A similar effect is shown with the number of discovered vulnerabilities (purple line), and the personnel's training level (yellow line). In these cases, less investment in vulnerability management leads to less discovered vulnerabilities and less investment in training means less accumulated training hours (units are in hundreds of hours). However, the training curve is slower because the hiring process is slower and the obsolescence of training is slower as well.

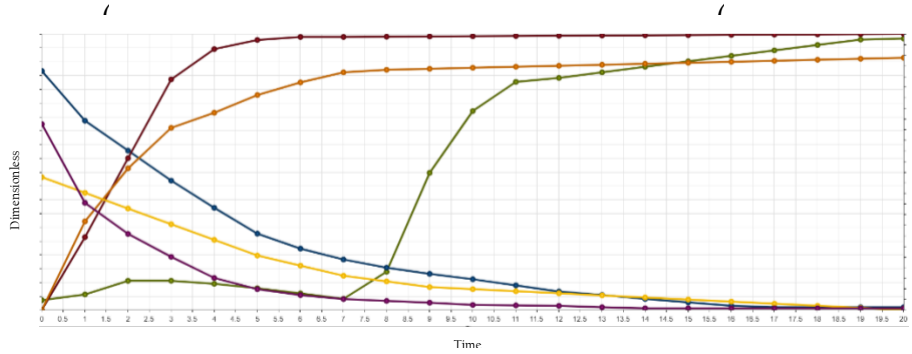

Figure 4.7 Detections (orange), false alerts (red), patched systems (blue), discovered vulnerabilities (purple), training (yellow) and impact (green) BoTs

While all of this happens, the company is under constant threats. Consequently, the model is designed to have a stable influx of threats and possible incidents. The high investment in detection avoids immediate high impacts, but the increase in false alerts does impact the company before it can stabilize and decrease the impact as shown in Figure 4.7 (green). However, this only works for a small amount of time. Later the lack of investment in protection and training to develop plans when there is a breach would increase the impact severely, as shown in Figure 4.7 (green). The experts anticipated that the impact would eventually start to stabilize because the possible damage is limited but could keep affecting the company further.

In all the mentioned variables, units and quantitative data could be used. However, due to the different circumstances companies could be in, it is impossible to calibrate a model that accurately represents all the companies that wanted to use it. In this sense, the given numerical values in the y-axes of the graphs were numbers used for calibration purposes but are not as relevant as the changes in shapes, inflections, maxima and minima in the graphs.

Moreover, this is one of the BoTs used to calibrate the model with extreme scenarios. Although the scenario could be a real strategy by a company it is likely that in real scenarios there is always a mix of different investments. However, the calibration of these extreme scenarios was used to determine the boundaries of the model with the experts as explained in the methodology (Section 3.5).

4.6.2 Graphical user interface

Using the described model and reference modes as a base, an interface for the decisions makers was developed as shown in Figure 4.8. When the decision makers open the interface, the input variables of the model are shown in sliders with a scale of 0-100%. In these sliders, the decision makers can allocate their budget until they complete a 100% total and click simulate. If the decision makers do not wish to allocate all the budget they can allocate as much as they want and click simulate.

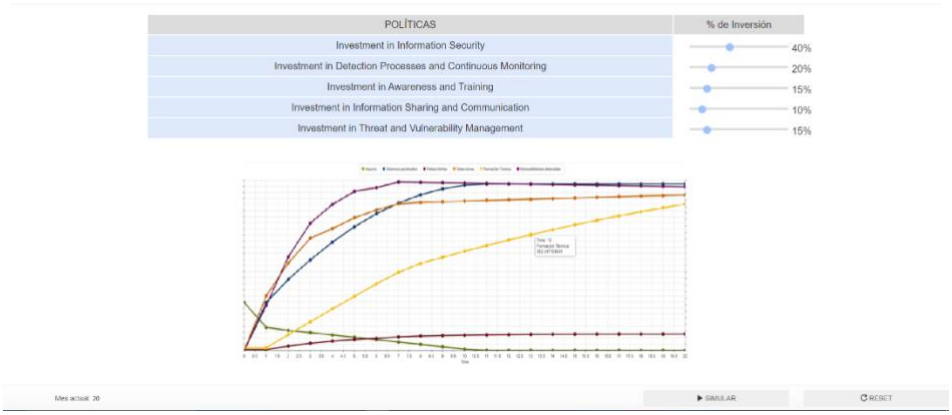

Figure 4.8 Cyber Range Interface

In the case of the previously described model there are five input variables. Hence, there are five sliders on the decision maker's screen to allocate budget to each one of them.

Furthermore, once the decision makers click on the simulate button a graph of the impact over the course of 20 months is shown on screen. The impact of cyber incidents over time will depend on the allocation selected by the decision makers and thus they will be able to re-adjust their decisions and experiment with different allocations and dynamic investment strategies to try to minimize the impact as soon as possible. In this process, the decision maker can learn the effects described in the model that are the theoretical interrelationships between cyber resilience policies. For instance, as shown in the reference behavior in the previous subsection where the decision maker allocates 100% of the budget to detection, they would find out that the impact increases with respect to the original situation after a slight decrease, because without the adequate training, the false alerts consume resources and time that cost money to the company. This effect is shown in Figure 4.9. As shown in the figure, the model and interface are capable of having similar behaviors than the reference mode described by the experts (shown in the green line in Figure 4.7).

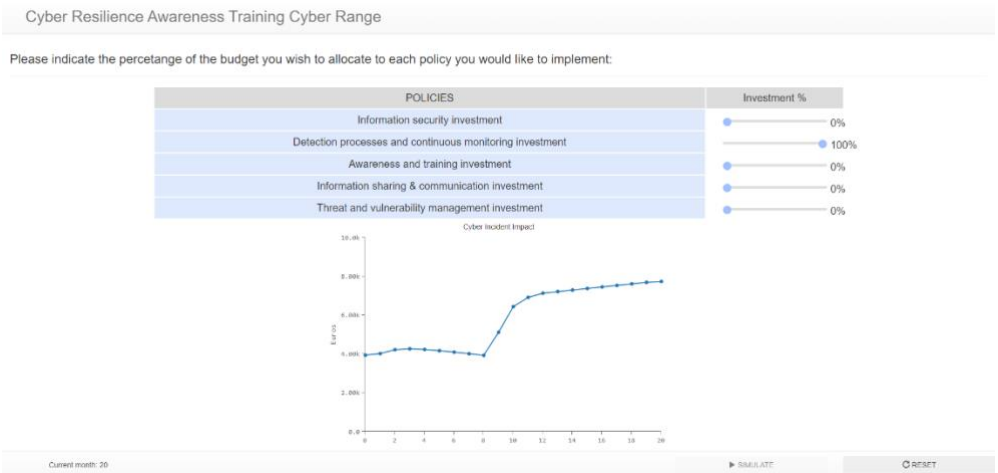

Figure 4.9 Allocating 100% of the budget to detection

As in this example, other theoretical behaviors of cyber resilience policies can be shown by the cyber range. Moreover, although this interface does not

show more variables, the interface could be designed to show more variables as indicators so that the decision maker has more hints to understand the consequences of their decisions.

4.7 Cyber Resilience Operationalization Framework (CR-OF)

The previously described results can all aid cyber resilience operationalization decision-makers in SMEs. These results aid in different ways, varying from choosing the actions or policies that an SME needs to implement to giving them an idea on how to continue their operationalization once they have started. A summary of these results is shown in Table 4.16.

Table 4.16 Summary of results and how they aid SMEs

Result	Description	Aid for SMEs
Conceptual Framework (CR-CF)	List and classification of domains and policies	Helps SMEs identify easily the essential cyber resilience operationalization policies and domains without prior knowledge of the documents in the literature.
Implementation Order	Example of chronological order for an effective implementation of cyber resilience policies.	Aids with prioritization of the cyber resilience policies.
Cyber Resilience Progression Model	Example of natural progression of policies	Lets SMEs identify the actions they can implement to continue improving their current cyber resilience implementation.
Cyber Resilience Cyber Range (CR)^2	Proposal of cyber ranges with SD models to explain interrelationships between policies	Increases the decision-makers' awareness on the importance of having a balanced cyber resilience investment and the complexity of the policies' interrelationships.
Self-Assessment Tool (CR-SAT)	Questionnaire to assess the current maturity.	Aids companies in the identification of their current situation in the progression model to identify the next steps.

The combination of the previously described results can be used to operationalize cyber resilience in a systematic manner. This combination has therefore become the main result of this thesis: a cyber resilience operationalization framework (CR-OF).

Inspired in the Plan-Do-Check-Act (PDCA) continuous improvement process, a systematic cyber resilience operationalization process can be applied

using the CR-OF. Figure 4.10 shows the systematic continuous improvement process that the CR-OF represents.

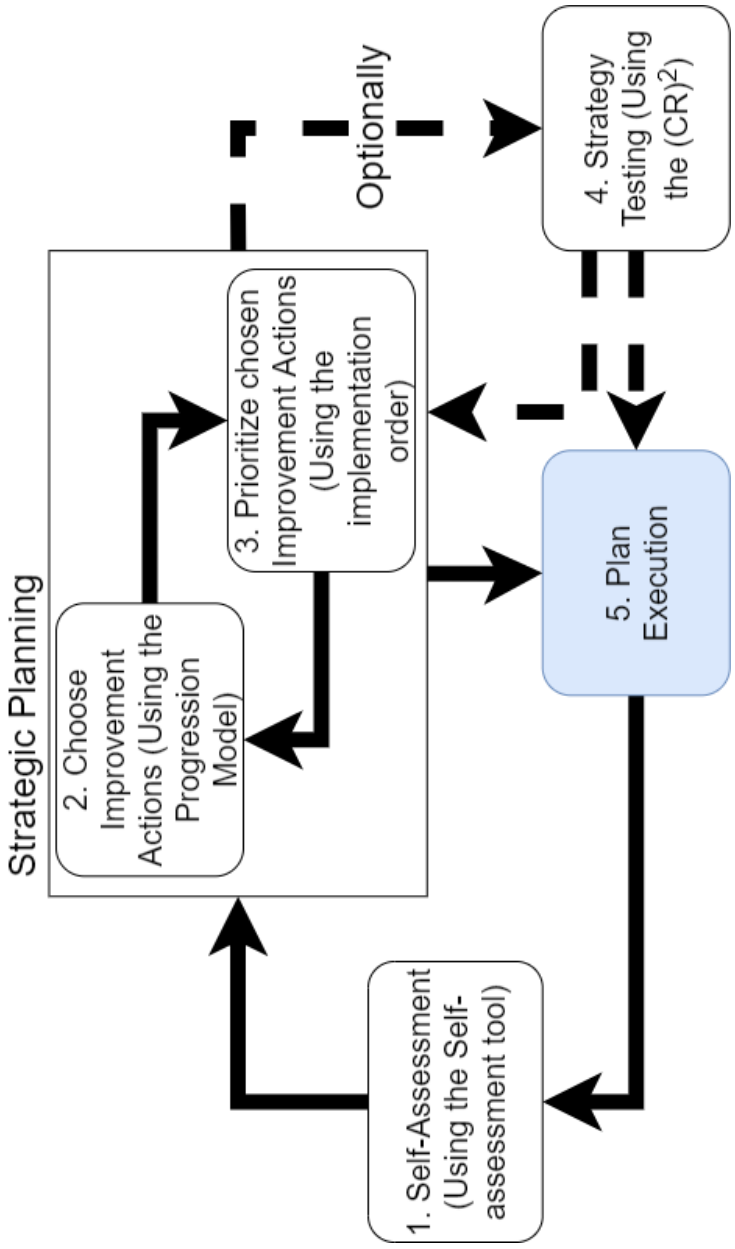

Figure 4.10 Systematic Cyber Resilience Operationalization Process

As the figure shows, the process starts with a self-assessment of the company's current cyber resilience operationalization. This self-assessment can be made with the self-assessment tool (CR-SAT). This would help the decision maker in charge of the cyber resilience operationalization (the end user of the CR-OF and its tools) understand the shortcomings of the currently implemented policies and based on these shortcomings be able to start a strategic planning phase in order to improve them. The strategic planning phase is composed of two processes that iterate. These processes are the identification of actions to improve the current cyber resilience operationalization and the prioritization of these actions. These two processes can be achieved by combining the descriptions in the progression model and the implementation order.

After the strategic planning the company can optionally test their strategy by using the simulation models and the $(CR)^2$ to understand the effects of the selected actions. Although this process is optional, iteration with the strategic planning processes would reinforce the understanding and knowledge of the decision-maker regarding cyber resilience operationalization.

Finally, the company can implement the plan that resulted from the previous steps. After this execution, the process can start again by assessing the new state of the cyber resilience operationalization in the company through the self-assessment tool. Similar to the PDCA, this process can be iterated to continuously improve in the cyber resilience operationalization and therefore in the cyber resilience capabilities of a company.

A generalization of the process companies would need to follow in order to use the described part of the CR-OF would have the following steps:

1. Self-Assess their current cyber resilience maturity in each policy (using the CR-SAT). Choose the policies in which they would like to improve based on the self-assessment.
2. If the company has policies in maturity levels considerably lower than their average maturity, prioritize improving those policies. Else, if the company has several policies to improve even after using that first criterion, use the implementation order to decide which one is more beneficial to prioritize.

3. Using the next maturity states' descriptions in the progression model, choose specific actions to improve the selected policies.
4. Optionally test their strategy with a cyber resilience cyber range. This would help the company understand the theoretical effects of their investments and test if their prioritization is correct. If necessary, the company could have to go back to the strategic planning (steps 2 and 3).
5. Execute the developed plan.
6. Go back to step 1.

For more detailed examples of how this process could be applied, see the next chapter (Chapter 5) and Appendix E.

5 Evaluation

This section presents a series of case studies used to qualitatively evaluate the cyber resilience operationalization framework (CR-OF). The aim of this evaluation phase is to assess the completeness and usefulness of the CR-OF. To that end SMEs and cybersecurity providers, the two types of stakeholders identified to be involved in cyber resilience operationalization, used the CR-OF and gave their feedback on it. This feedback was regarding whether they thought that the CR-OF had everything needed to operationalize cyber resilience (completeness) in SMEs and regarding whether they believed the CR-OF would help them follow a process of evaluation of their cyber resilience selection of improvement actions, and prioritization of said actions (usefulness).

5.1 Case Studies

As described in the methodology chapter, several case studies were used to ascertain the completeness and usefulness of the CR-OF. These case studies were chosen with the criterion of having less than 250 employees, a broad definition for an SME. The other criteria used to choose the case studies was to try to include variety in either their size among the SME criterion (companies with different employee counts) or the context (geographical location, sector, etc.).

During these case studies, the participating SMEs were able to use the CR-OF to self-assess their current cyber resilience, find improvement actions and prioritize them through the implementation order. The following subsections describe the contexts of each organization and their results after the case study while a broad summary is shown in Table 5.1.

In each of the following case studies, there is a brief description of each company, its context and its current evaluation. After this, there is a table that summarizes their current maturity state in each domain, the evidences they found for selecting that maturity level, and the actions they identified as appropriate to improve in each domain. To see the complete process followed by each company and where the summary tables come from, Appendix E shows a complete description of one of the case studies (the paint manufacturer company from Spain).

Table 5.1 Case study results' summary

Case	Number of employees	Sector	Country	Average cyber resilience maturity state
Port-logistics company	150	Logistics	El Salvador	2.61
Paint manufacturer	200	Industrial	Spain	3.27
Clinical pharmacy organization	30	Services	USA	3.79
Machine tool manufacturer	225	Industrial	Spain	2.54
Machine tool manufacturer II	150	Industrial	Spain	2.46
Mold Manufacturer	50	Industrial	Spain	2.25

5.1.1 Port Logistics Company from El Salvador

The first conducted case study was made in a port logistics company with 150 employees located in one of the main maritime ports in El Salvador. Due its activity, the company has to deal with imports and exports of different types of cargo. The main type of cargo the company receives is merchandise imported to El Salvador to be used as raw material or to be sold in the country. This activity is strictly regulated by the local government and other international organizations such as the International Maritime Organization (IMO). According to the evidences expressed during the communications with the CTO of the company and the triangulation with other sources [135], this regulation strongly influences the way this company handles cyber resilience.

Up to this moment, the company does not report to have suffered any kind of cyber incident. As the literature suggests, this is also an influencing factor on the awareness of the management and therefore, their willingness to invest in cyber resilience policies [136].

Considering these factors as the current context of the company, the evidence collected during the case study suggests that the company is in an intermediate level of cyber resilience operationalization with an average state across the 10 domains of 2.61 (over 5).

Figure 5.1. shows the radar graph with the average state in each of the 10 domains. As shown by the graph the company has the most maturity in the Asset Management domain, and the least in the Awareness and Training domain.

During the case study, the company's CTO was able to identify a fitting state in each of the cyber resilience policies and support it with evidences. Moreover, this decision maker was also able to identify actions to improve the company's cyber resilience. The summary of the evidences and identified actions per domain is shown in Table 5.2.

As evidenced by the case study, this company has an intermediate level of cyber resilience mostly motivated by the compliance with regulation. Their most advanced domain was asset management, indicating that this company has prioritized correctly in the initial stages of cyber resilience operationalization according to the implementation order proposed in this thesis (Chapter 4, Section 4.3). The same thing happens with Incident Analysis, but the evidences for this domain were mostly based on experience with safety incidents and these might not translate as effectively to cyber resilience. Using the implementation order, the company was able to prioritize the identified actions and decided that their next steps have to focus on formalizing the risk management, especially regarding the definition of a risk tolerance threshold in order to correctly define budgets for cyber resilience management. Afterwards, they considered that they should focus on the mitigation of risks, threats and vulnerabilities, and thus, improve their information security, business continuity management and other domains that help mitigate these threats, vulnerabilities and risks. To support these improvements, the company considered that they needed to enhance their training and awareness, since this is a domain that contains transversal aiding policies [137] that can overall improve the cyber resilience operationalization in the company.

Therefore, this case study has evidenced that this company has been able to identify correct actions to effectively improve their cyber resilience and prioritize these actions.

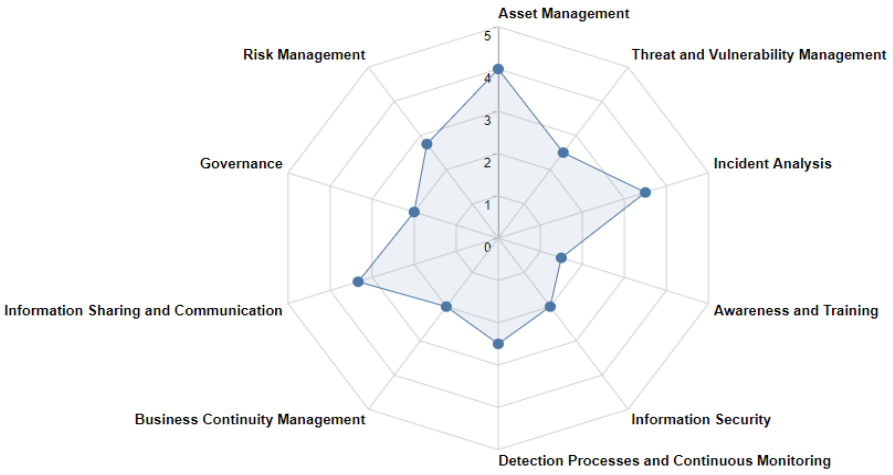

Figure 5.1. Domain-level overview of the port logistics company from El Salvador

Table 5.2 Summary of evidences and identified actions per domain in case study 1

Domain	Implementation State	Summary of Evidences	Identified Actions
Governance	2.00	The company's strategy is widely influenced by the regulation around it which includes local laws and the regulation and guidance from the IMO. The strategy is still passive, but their compliance with the regulation has improved their situation. The current allocation of resources is not specific for cybersecurity but shared with the IT budget.	Start defining specific budgets for cyber resilience operationalization. Define a proactive strategy that goes beyond compliance with regulation.
Risk Management	2.75	There are risk management processes in place in the company due to safety and external regulation. These general processes have helped the company identify risks, classify and prioritize them. Priorities on safety and compliance have led to a stale situation with the mitigation of cyber risks.	Define a risk tolerance threshold based on an acceptable level of risk quantity (probability x impact). Start using part of the cyber resilience budget to mitigate cyber risks that exceed the risk tolerance threshold.
Asset Management	4.00	There is rigorous control of the inventory of assets with detailed lists of assets and correctly documented in a database. Due to a lack of specific budget, maintenance of the assets and the traceability of changes are still passive with mostly corrective maintenance and not much control over the changes. However, there seems to be initiative in both fronts as they have started both, preventive maintenance on occasion and the control of changes (still without traceability).	The company saw it more relevant to improve other domains since this was their highest, so no actions were identified in this domain.
Threat and Vulnerability Management	2.50	There is awareness of technical vulnerabilities due to the experience of the IT department's personnel, but the technical vulnerabilities are mainly handled in an intuitive manner. The mitigation of these vulnerabilities is similar to the risk mitigation, where only the most important vulnerabilities are mitigated or the ones required by regulation.	Start identifying threats and vulnerabilities in a more proactive way. Classify them and include them in the risk management.
Incident Analysis	3.50	There is no experience in the company of past cyber incidents. However, their vast experience with safety incidents leads them to believe that the analysis of the situation would be handled similarly. They would evaluate the damages and losses,	The company saw it more relevant to improve other domains, so no actions were identified in this domain.

		do a forensic investigation to determine what happened and try to adopt measures to avoid this from happening again.	
Awareness and Training	1.50	There are no plans in the company for awareness and training. In the company only the IT personnel gets training regarding cybersecurity and basic cyber risk awareness is communicated occasionally for the rest of the personnel through e-mails.	Define at least one general training and awareness plan for the personnel.
Information Security	2.00	The most basic measures to protect confidentiality are in place (mostly access control), but permission control is still separated from the objectives set in the strategy due to the lack of proactivity in the latter. Integrity protection is basic and aligned with the confidentiality measures. The availability is their most protected front with multiple automatic backups that can be recovered in case of an incident. These backups are made weekly with a commercial solution.	Improve confidentiality measures by monitoring the implemented measures of permission control, i.e. make sure that only authorized personnel can access and modify protected information.
Detection Processes and Continuous Monitoring	2.50	There is a SIEM in place to monitor the most important assets in real-time. The plans in case of a detection are undocumented and consist primarily on calling the IT personnel who should try to respond.	Start paying more attention to the monitored indicators. Document at least one general plan in case of the detection of a cyber incident.
Business Continuity Management	2.00	There are no documented plans, the IT personnel has ideas of what they would do to respond in certain situations. These ideas have not been tested.	Document the plans in the IT personnel's mind.
Information Sharing and Communication	3.33	Relationships with the local government, local police and the IMO are well defined and geared towards the collaboration in cybersecurity intelligence. However, due to the wide variety of clients (ranging from individuals to multinational companies) there are only informal relationships with external stakeholders such as clients.	The company saw it more relevant to improve other domains, so no actions were identified in this domain.
OVERALL	2.61		

5.1.2 Paint Manufacturer from Spain

The second conducted case study is a 200-employee paint manufacturing company from the Basque Country, Spain.

The Basque Country is one of the most industrialized regions in Spain. For this reason, the regional government has strategic focus on promoting industrial cybersecurity. Thus, the region has two cybersecurity centers of their own [135], [138] as well as the Spanish national authorities and cybersecurity institute as aids to improve their cybersecurity [139]. Due to the strategic focus on cybersecurity in the region, the government has promoted and recommended the aid of cybersecurity providers to local companies [140].

Moreover, this company has suffered two cyber incidents in the past two years, leading to an increase of awareness and the increased emphasis in protecting their systems through the outsourcing of certain cybersecurity services.

Considering the context of the company, their recent experiences with cyber incidents, the evidence collected from the case study suggests that they have an average cyber resilience state of 3.27 (over 5). The summary of their average state in each cyber resilience domain is shown in the radar chart in Figure 5.2. As shown in the figure, the company has the most maturity in the Incident Analysis domain and the least in Business Continuity Management.

During the case study, the company was able to identify a fitting state in each of the cyber resilience policies and support it with evidences. The summary of the evidences provided and the improvement actions identified per domain are shown in Table 5.3.

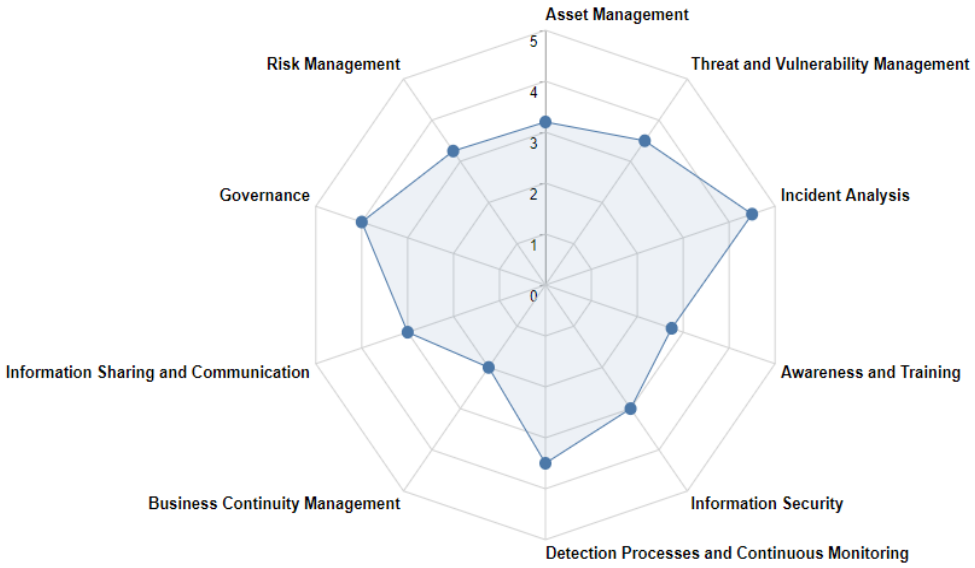

Figure 5.2 Domain-level overview of a paint manufacturing company from Spain

As shown in the evidences of this case study, the use of outsourcing has influenced and improved the way this company manages cyber resilience operationalization. Another important factor in their improvement has been the increase of awareness developed from the experience of the suffered cyber incidents. In fact, their most advanced domain was Incident Analysis, especially because they have been able to learn from their past incidents and improve their cyber resilience through these experiences.

However, as evidenced by the low maturity in Business Continuity Management this company is still focused on a cybersecurity point of view in which protection and prevention strongly prevail over the investment in business continuity (responding and recovering) which means the company is trying to become fail-safe. In addition, the outsourcing of cybersecurity services has led to a lower level of Awareness and Training, their second lowest maturity amongst the cyber resilience domains.

Table 5.3 Summary of evidences and identified actions per domain in case study 2

Domain	Implementation State	Summary of Evidences	Identified Actions
Governance	4.00	Since the company suffered two cyberattacks, the management decided to invest heavily on securing their assets. The board meets at least once every year to discuss their cyber resilience strategy and improve it according to their experience in the year.	The company decided to prioritize other domains since this is one of their most advanced ones.
Risk Management	3.25	Their cybersecurity provider is managing their risks. To the company's knowledge, risk is not quantified as a function of probability and potential impact, but with their cybersecurity provider, they consider the potential impact when deciding to mitigate a risk. Their knowledge and classification of risks is limited to what their provider shares with them. The company does not have a risk tolerance threshold defined at the moment.	Start quantifying risks as a function of probability and potential impact. Define and use a risk tolerance threshold to make informed decisions when mitigating risks.
Asset Management	3.20	The company has the invoices of the systems that they have bought throughout the years. If needed, they consult these invoices as a sort of detailed asset list since these invoices contain all the information from their assets. The company outsources their IT services such as configuration and change management. They also periodically do preventive maintenance on their systems and have a list of the interdependencies between their systems because of their relatively low number, but do not know the external dependencies.	Compile the invoices into a detailed, ordered list or database to have an easier access to it. Include the dependencies between assets in this list.
Threat and Vulnerability Management	3.50	Similar to the risk management domain, the cybersecurity provider is the one in charge of managing threats and vulnerabilities. They send the company informative bulletins with the latest vulnerabilities to their systems, but do not systematically find every vulnerability in their systems. The mitigation is based on potential impact to the company.	Systematically identify threats and vulnerabilities already existent in the systems. Classify and prioritize these vulnerabilities to patch them as needed according to the same criteria as risks.

Incident Analysis	4.50	The company has been able to improve their analysis and learn more from their second incident compared to their first. They have also improved their analysis of the situation and their forensic analysis. They hired a company to do a full forensic analysis on the last incident; this analysis was sent to the authorities.	Since this is currently their best domain, the company decided to focus on the improvement of other domains.
Awareness and Training	2.75	There is a general technical training plan for the IT personnel and occasional awareness communications for employees sent through e-mail.	Create plans according to the different profiles in the personnel and their cyber resilience-related activities. Formalize awareness training for the personnel.
Information Security	3.00	The company has permission control software that monitors the activity of restricted data (mostly clients' personal data) so that only authorized personnel can access that data. Integrity is not specifically addressed. Availability is managed through multiple backups including a physical backup done daily and that the CEO takes that home every day.	Encrypt the data from the physical hard drive in case it is lost.
Detection Processes and Continuous Monitoring	3.50	There is a SIEM installed in the company that is managed by the cybersecurity provider. The SIEM generates automatic alerts on the event of any anomaly. There is a general detection process in which the local police and the IT personnel are informed as soon as possible.	Formalize the current detection process in a document and communicate it to the personnel and cybersecurity provider. Develop specific detection processes for different types of incidents.
Business Continuity Management	2.00	Despite their experiences with previous incidents the company only keeps in mind their action plans when something happens and has never tested these plans. The multiple backups of information have never been tested to see if they can be restored.	Test the backups of information, especially the physical one that is taken outside of the facilities every day.
Information Sharing and Communication	3.00	There are no formal collaboration agreements with external stakeholders or entities. The only communications have been with authorities when they have suffered incidents. They had the initiative to share information with clients when they had the last incident to warn them about the threat they faced, but ended up not sending anything.	Formalize the information sharing they currently have into agreements with their clients and other entities.
OVERALL	3.27		

Their overall average cyber resilience maturity state suggests an already advanced cyber resilience operationalization. Their prioritization up to this date seems correct and coherent to the implementation order (Figure 4.2) with a deep knowledge of their assets, their risks and thus an informed strategy and correct measures.

The next steps for this company, as identified by themselves, are to formalize certain cyber resilience policies that are already in place such as risk management with the proper quantification of risks. On the other hand, start improving their Business Continuity by documenting and testing their response and recovery plans. Improve their Awareness and Training plans as a way to support their other cyber resilience operationalization policies that are already in place. And, finally, to gradually improve the rest of their implemented domains and policies. As shown in the radar chart in Figure 5.2, this company has, in general, a well-balanced cyber resilience with similar states in most domains. This means that the company has diversified their investments and not focused on only one domain as the solution. This dynamic investment strategy is crucial to the cyber resilience building process and an effective cyber resilience operationalization [136].

5.1.3 Clinical Pharmacy Organization from the USA

The third case study conducted for this thesis was in a clinical pharmacy organization with base in Florida, USA. This company's main activity is to consult medical insurance companies with risk management programs and solutions. Due to its nature, the company manages large amounts of information from patients' insurance information which in the United States is protected under the Health Insurance Portability and Accountability Act (HIPAA), a law that requires special care with this kind of information. Besides the compliance with HIPAA requirements, the company from this case study is ISO 27000 certified and follows the HITRUST cyber security framework guidelines without having an official certification due to the cost of a HITRUST certification.

The company has not yet suffered a breach of information but has suffered minor incidents regarding misuse of cyber equipment (e.g., miss-spelling names) which, due to their activity, they classify as an incident and have had to document these incidents and their respective corrective actions as required by the ISO standard.

Considering this context and its influence on the company, the overall average maturity level of the company is a 3.79 (over 5). The summary of their average state in each cyber resilience domain is shown in the radar chart in Figure 5.3. As shown in the figure, this company is very balanced in general, but has the most maturity in the Information Sharing and Communication domain and the least in the Awareness and Training domain.

During the case study, the company's members were able to identify a fitting state in each of the cyber resilience policies and support it with evidences. The summary of the evidences the company provided and the improvement actions they identified per domain is shown in Table 5.4.

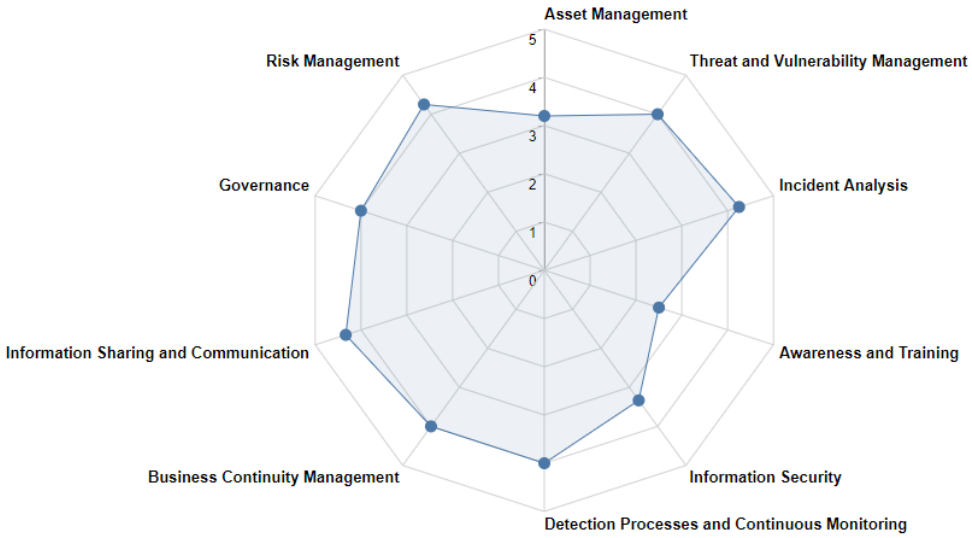

Figure 5.3 Domain-level overview of a clinical pharmacy company from the USA.

Table 5.4 Summary of evidences and identified actions per domain in case study 3

Domain	Implementation State	Summary of Evidences	Identified Actions
Governance	4.00	The company is certified in the ISO 27000 and follows the HITRUST[2] cybersecurity framework so they have implemented an information security management system as a strategy to improve their cyber resilience. Although they comply with ISO the company feels like they could do more to continually improve their strategy. The company also has to comply with HIPAA and other laws regarding the protection of health information from their clients.	The company has been motivated by compliance to achieve its current state in the governance domain but feels like they could start putting more effort into the continuous improvement of the strategy. They would also like to start to research more strict regulations that might help them improve their current security.
Risk Management	4.25	There is a systematic and documented procedure to identify and classify risks on a risk matrix. They use colors in the risk matrix in the form of a heat map to easily identify the risks that are unbearable for the company. Their mitigation is mostly directed towards avoiding breaches since for them it would mean so many costs due to HIPAA that they would probably go bankrupt.	Since this is one of the most advanced domains, the company has decided to prioritize others.
Asset Management	3.20	The inventory of the company is highly detailed and documented as ISO 27000 requires. Preventive maintenance is not programmed but rather occasional since it means stopping their service to patients for the time the maintenance lasts. There is no control of dependencies in the systems, the company believes there are not many dependencies because of the few systems they have.	The company has decided to program their preventive maintenance to avoid as many problems as they can through the update and maintenance of their systems. They have also decided to start managing the configurations of their systems through a CMDB.
Threat and Vulnerability Management	4.00	The company outsources the monitoring of vulnerabilities and the evaluation of their cybersecurity measures and for this reason carries out penetration testing at least once a year, researches the vulnerabilities of their assets at least once a month. Vulnerabilities that might cause a breach (i.e. that are perceived as priorities) are mitigated.	The company has decided to improve this domain by starting to mitigate vulnerabilities in a more systematic way rather than just the vulnerabilities that could lead to a breach.

[2] More information about HITRUST CSF available at: https://hitrustalliance.net/product-tool/hitrust-csf/

Incident Analysis	4.25	Due to HIPAA the company is required to do a very complete forensic analysis whenever something happened and report it to the authorities. Due to the ISO standard they would require to evaluate their response, document the lessons learned and implement them in future incidents.	Since this is one of the most advanced domains, the company has decided to prioritize others.
Awareness and Training	2.50	Since the company outsources most of the technical cybersecurity measures their awareness and training is mostly focused on sending periodic reminders of the basic measures everyone has to follow. These communications are mostly related to awareness training and not technical training which is very general and only for a few members of the personnel. The company tries to hire only personnel that already comes with the needed technical training for their tasks.	The company should define technical training plans more specific to the needs of the personnel. The current knowledge of cybersecurity in the company is very limited due to the focus on awareness. The company has also identified the need to start evaluating the current knowledge of the personnel to define these training plans.
Information Security	3.33	Due to the nature of the company their focus is on confidentiality of the data that they collect for their services. Therefore, the company has very advanced confidentiality measures. The company also uses a Rackspace Commvault system for backups in a very secure infrastructure provided by this commercial solution.	The company has decided to improve their integrity measures since they have no specific controls to avoid tampering other than those of the confidentiality measures and their monitorization.
Detection Processes and Continuous Monitoring	4.00	The company has an installed SIEM and an outsourced company that monitors and acts accordingly when the SIEM detects anomalies. The company also has a documented general plan for what to do in case of a detection, however this plan relies on calling the authorities and following the instructions from authorities and their outsourced company's instructions.	The company feels like they need more information out of their provider and want to either change the provider or do an in-site management of this domain.
Business Continuity Management	4.00	The company has documented plans for response and recovery due to the importance of certain incidents such as a breach. HIPAA requires the definition of contingency plans for such incidents. In the company, these plans have been tested to ensure they would maintain the business continuity.	Business continuity plans are very well defined, have been tested and comply with HIPAA and thus the company has decided to prioritize other domains.
Information Sharing and Communication	4.33	The company has formal collaboration with other entities to share information. Their clients are part of their cybersecurity strategy since in some cases these clients audit them. The emergency communication plans are in compliance with HIPAA requirements.	This is the company's best domain at the moment, so they have decided to prioritize others.
OVERALL	3.79		

As shown in the evidences of this case study, there are multiple factors that have influenced the current cyber resilience state of the company. The most important of these factors is compliance since the company is very driven by the compliance to HIPAA and the compliance to the ISO 27000 standard. On the other hand, the company has outsourced part of its cybersecurity activities such as the monitoring and has commercial technical solutions for others (such as backups) that make these tasks automatic. The nature of the data the company works with has made them work on their resilience to cyber incidents since their main activity is related to the management of this important data. Hence, their high maturity state in the Information Sharing and Communication domain due to the auditing from the clients and collaboration with authorities.

The least developed domain in the company is Training and Awareness, which can be explained by their lack of internal management of cybersecurity. This company invests heavily on cybersecurity solutions and outsourcing and with only 30 employees to develop its activity, the training related to cyber resilience is not in their priorities. Thus, the only training the employees receive is the basic awareness training related to not clicking on spam e-mails, having a strong secure password, etc.

As mentioned before, this company seems overall balanced with most domains close in maturity state. In addition, the company is more advanced in most cyber resilience policies compared to the previous case studies. However, the company was able to self-asses using the CR-SAT and identified correct actions to improve their cyber resilience. To further improve in their cyber resilience, the prioritization of the actions they considered for improvement starts in the asset management domain, by improving their configuration and change management. They also considered they do not have too many corrective maintenance cases, but that they periodically update their systems as a way of preventive maintenance to help them keep systems patched against possible vulnerabilities. They also considered an improvement in awareness and training to be necessary to help the company better understand the measures they are implementing and make them more effective. Especially if they absorb certain cybersecurity tasks, such as monitorization, with which they are not satisfied. They consider the development of technical training plans for the personnel who

will be in charge of these tasks to be essential in their success with this absorption.

5.1.4 Machine tool manufacturer from Spain.

The fourth conducted case study is a 225-employee machine tool manufacturing company from the Basque Country, Spain.

As mentioned previously, the Basque Country is one of the most industrialized regions in Spain and due to the high value of the industry in the region, the government has strategic focus on promoting industrial cybersecurity.

Moreover, the Basque Country has several wide network of cooperative society groups. These companies owned by the employees have grown to be very relevant in many sectors of the industry. The company in this case study is a cooperative society with many "sibling" companies that, according to their IT manager, work in the same way regarding cybersecurity.

This company is also in a transition stage starting to formalize the cyber resilience implementation by defining a "cybersecurity master plan" or what in the context of this research has been broadly defined as a cyber resilience strategy. Therefore, the company pointed out that they are more curious to see their results in the long term regarding their self-assessment to see the effects of their actions.

Considering this context and its influence on the company, the overall average maturity level of the company is a 2.54 (over 5). The summary of their average state in each cyber resilience domain is shown in the radar chart in Figure 5.4. As shown in the figure, this company has the most maturity in the Threat and Vulnerability Management domain and the least in the Governance domain.

During the case study, the company was able to identify a fitting state in each of the cyber resilience policies and support it with evidences. The summary of the evidences they provided and the improvement actions they identified per domain is shown in Table 5.5.

.

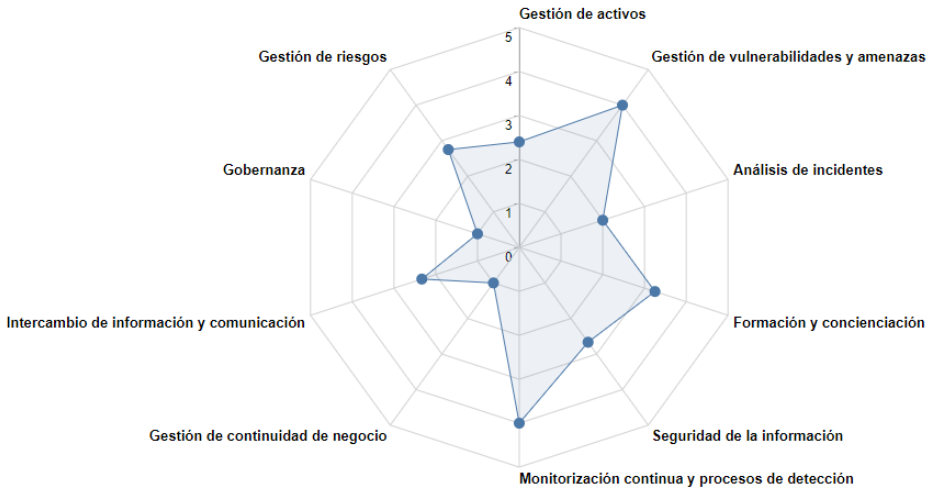

Figure 5.4 Domain-level overview of a machine tool manufacturer in the Basque Country

As shown in the evidences of this case study, this is another instance where the Basque Government's initiative to promote the collaboration with cybersecurity providers has improved the cyber resilience of a company. By collaborating with different cybersecurity providers this company has been able to monitor their assets and identify their threats to try to minimize the risks of having incidents. Up to this point, this strategy has proven useful since they know of similar companies nearby that have suffered cyberattacks that they have been able to avoid.

However, similar to the case of the paint manufacturer in case study 2, the low maturity in Business Continuity Management indicates that this company is still focused on a cybersecurity approach in which protection and prevention strongly prevail over the investment in business continuity (responding and recovering) which means the company is trying to become fail-safe. In this case, however, the awareness and training domain has not been neglected.

Table 5.5 Summary of evidences and identified actions per domain in case study 4

Domain	Implementation State	Summary of Evidences	Identified Actions
Governance	1.00	The company has no defined cybersecurity strategy and the budget for cybersecurity implementation comes from the IT budget. At the moment, the company is not aware of any other regulation other than the GDPR that applies to their activity and they only comply with this one.	Define a cybersecurity driver plan. Their intention is that the cybersecurity plan serves as a strategy with objectives, priorities, budgets and responsibility allocation.
Risk Management	2.75	The company makes a risk matrix that matches each of their internal services to the risk they are exposed to. They compromise their risk tolerance threshold in meetings with the company's management board.	The company wants to improve by reviewing the risk matrix annually.
Asset Management	2.40	The company has a very thorough inventory of hardware and software they have recently used this documentation to plead their case against a software provider that claimed they had more licenses in use than they really had. This inventory is made automatically every 6 months. For configuration and change management the company uses generic patterns for each type of asset.	To further improve this domain the company decided to work on dependency management. The IT director considers this important for maintenance-related activities and continuity management.
Threat and Vulnerability Management	4.00	The company does an exhaustive vulnerability identification once every two years with Penetration Testing done by an external company. Every month they also receive alerts on newly discovered vulnerabilities that could affect their systems. They follow up on the discovered vulnerabilities thoroughly and try to remove any vulnerability that is higher than the risk tolerance threshold.	Since this is one of their most advanced domains, the company has decided to prioritize others.
Incident Analysis	2.00	The company has not suffered any significant incidents, but in case of an incident they assess the damages caused by it and try to implement the measures to avoid the same type of incident happening again.	Since the company has no experiences with incidents they do not have plans to improve this domain at the moment.
Awareness and Training	3.25	There are defined training and awareness plans that although not documented are followed to train employees and these plans are prioritized depending on the tasks the employee performs in the company. The emphasis of these plans is in awareness and especially	The company wants to hire new people with specialized knowledge in cybersecurity and also make phishing simulations to evaluate the results of the training they are imparting.

		for the employees that manage bank accounts or the company's money in any other way.	
Information Security	2.67	The company has a well-defined access control with a permission management. They also have an automatic backup system that takes around 10 snapshots per day and a redundancy system that has real-time data processing centers replication.	Due to their very advanced availability measures that also ensure the possibility to recover in case of incidents, the company did not prioritize this domain for improvements.
Detection Processes and Continuous Monitoring	4.00	The company uses NAGIOS software for a strict monitoring of assets. This software lets them monitor everything from screens located in the IT department.	Since this is one of their most advanced domains, the company has decided to prioritize others.
Business Continuity Management	1.00	The company only intuitively has the recovery plans that involve the backups that they make automatically. These plans are not tested and there are no response plans whatsoever.	Define incident-specific plans for the most common types of incident. These plans have to include and test the plans that involve the current back-up system.
Information Sharing and Communication	2.33	The company has formal collaboration relationships with defined sharing policies with their stakeholders (suppliers, clients, cybersecurity provider, etc.) and certain other companies in their environment. This is enhanced because they are a part of a family of cooperative societies.	The company wants to improve their emergency communication plans in line with their improvements in business continuity.
OVERALL	2.54		

Their overall average cyber resilience maturity state suggests an already advanced cyber resilience operationalization. However, their prioritization up to this point has not been the best because they have focused on implementing protection and detection tools before defining a strategy with objectives, priorities and budgets. This type of prioritization up to this point can lead to ineffective protection of the critical assets.

On the other hand, after using the tool, the company was able to define their next steps in their cyber resilience operationalization. The steps they identified are to define a cyber resilience strategy (in the shape of a cybersecurity driver plan). Start improving their Business Continuity by documenting and testing their response and recovery plans. Finally, to gradually improve the rest of their implemented domains and policies by formalizing and documenting them, and making them more systematic. These steps are consistent with the implementation order in the CR-OF and seem to be well chosen considering the current maturity of the company. After defining a good strategy they will probably require adjustments to their current protection measures, but overall, their protection will be better because it will target their specific requirements according to their strategy.

5.1.5 Machine tool manufacturer II from Spain.

The fifth conducted case study is a 150-employee machine tool manufacturing company from the Basque Country, Spain. This company is a direct competitor of the company in the previous case study and thus shares most of its context. However, this company reports almost double the benefits. Despite the company not being a cooperative society they are part of a group of "sibling" companies that work together to expand their business horizontally.

Considering this context and its influence on the company, the overall average maturity level of the company is a 2.46 (over 5). The summary of their average state in each cyber resilience domain is shown in the radar chart in Figure 5.5. As shown in the figure, this company has the most maturity in the Information Sharing and Communication domain and the least in the Awareness and Training domain.

During the case study, the company's members were able to identify a fitting state in each of the cyber resilience policies and support it with evidences. The summary of the evidences they provided and the improvement actions they identified per domain is shown in Figure 5.5.

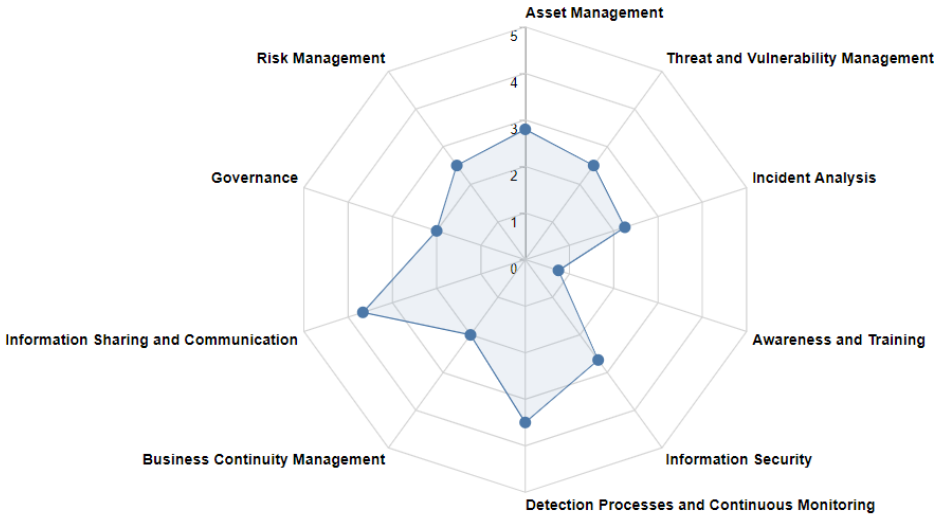

Figure 5.5 Domain-level overview of a machine tool manufacturer II in the Basque Country

Table 5.6 Summary of evidences and identified actions per domain in case study 5

Domain	Implementation State	Summary of Evidences	Identified Actions
Governance	2.00	There is a risk-oriented cybersecurity strategy in the company. Therefore, this strategy is mostly based on protecting their systems from identified threats and risks.	The company wants to improve their strategy by formalizing it in a document and centering it on the business continuity plans. As they see it, this would help them improve their risk management, asset management, detection processes and business continuity.
Risk Management	2.50	The company's IT department controls the risks that they consider priorities based on their experience and their knowledge of their business and assets.	The company wants to do a more systematic analysis of the risks by identifying the risks their assets are exposed to, classifying them and implementing a periodical systematic process to do so rather than doing this intuitively.
Asset Management	2.80	The company has an inventory of their assets, control the configurations informally and have an intuitive knowledge of the dependencies. They also maintain assets periodically and preventively by maintaining them updated as soon as any updates or patches come out.	In line with their business continuity strategy the company wants to improve their dependency management since it is useful to define response and recovery plans in an informed manner.
Threat and Vulnerability Management	2.50	The company identifies the vulnerabilities of their systems intuitively based on their current knowledge. They also receive information about their vulnerabilities occasionally from cybersecurity providers. They mitigate the identified vulnerabilities and threats when they identify them.	Just like for the risk management domain, the company mainly wants to formalize threat and vulnerability management by doing a systematic procedure to identify and mitigate vulnerabilities in a set period. In this case they have considered penetration testing yearly.
Incident Analysis	2.25	The company tries to identify as much information as possible after suffering an incident. Although they haven't suffered any significant incidents they have tracked minor ones to identify the damages, the causes, points of entry, methods, etc. The company has used this information to try to avoid the occurrence of these incidents.	The company wants to improve their incident analysis by evaluating their responses and decision making after every incident. According to them, this might help them improve their future decision making and let them learn more about each incident and prevent it from happening again.
Awareness and Training	0.75	The company only trains IT personnel in the necessary knowledge of cybersecurity they need to do their daily tasks. This training is not documented and mostly informal.	The company has decided to start doing periodical awareness training for all the employees and document a training plan for the IT personnel.

Information Security	2.67	The company has a permission management system in place and a backup system to ensure the availability in case of an emergency. They also have redundancies implemented to ensure availability of the most critical systems.	The company wants to improve in this domain by monitoring their confidentiality measures. They wish to introduce a software to be able to tell if the permission management is being forced on users and alert them in case of any unusual activity.
Detection Processes and Continuous Monitoring	3.50	The company has advanced monitoring that includes working with a cybersecurity provider who offers them monitoring services through a Security Operations Center. Internally they also have some monitoring capabilities and they check on live indicators of the states of various systems.	Since this is one of the most advanced domains in their evaluation, the company has decided to prioritize others.
Business Continuity Management	2.00	The company has an intuitive plan to respond and recover in case of an incident. This plan has not been tested and is not documented. Thus, the company is worried it might be too generic and not help them when they actually suffer an incident.	The company wants to define and document response and recovery plans that are adapted to every type of incident they can identify. They also want to test the most important plans to ensure they work in an emergency.
Information Sharing and Communication	3.67	The company has formalized cybersecurity collaboration with multiple cybersecurity providers and other external companies. Most of the external companies are due to their horizontal expansion through sibling companies that have formed a group.	Since this is one of their most advanced domains, the company has decided to prioritize others.
OVERALL	2.46		

As shown in the evidences of this case study, this company has received help from cybersecurity providers that have helped them improve several cyber resilience domains such as Continuous Monitoring and Detection processes. However, like in the second case study, this company has substituted the awareness and training of their personnel with cybersecurity providers and the implementation of protective technologies.

Their overall average cyber resilience maturity state suggests that the company has worked on the basic cybersecurity measures but has only started to formalize cyber resilience processes and policies. Despite this, for their maturity, their prioritization has been accurate with high emphasis on the balance between asset management, risk management, threat and vulnerability management and governance. This indicates that they are on the right direction according to the implementation order presented in the CR-OF and that the mitigation measures they have implemented are based on an informed strategy.

The next steps for this company, as identified by themselves, are to define training plans for the personnel. They want to put an emphasis on the awareness training for non-technical personnel since it is in this regard where they have not worked in the past, and they consider important. Moreover, they want to start improving their Business Continuity by documenting and testing their response and recovery plans. In their mindset, adjusting their strategy to focus on this domain will improve their governance, business continuity management, risk management, and several other domains.

5.1.6 Mold manufacturer from Spain.

The sixth conducted case study is a 50-employee mold manufacturing company from the Basque Country, Spain. Although not a competitor of the previous two case studies' companies, this company shares the context since it is also part of the Basque Country's industrial network.

Considering this context and its influence on the company, the overall average maturity level of the company is a 2.25 (over 5). The summary of their average state in each cyber resilience domain is shown in the radar chart in

Figure 5.6. As shown in the figure, this company has the most maturity in the Risk Management domain and the least in the Incident Analysis domain.

During the case study, the company's members were able to identify a fitting state in each of the cyber resilience policies and support it with evidences. The summary of the evidences they provided and the improvement actions they identified per domain is shown in Table 5.7 .

.

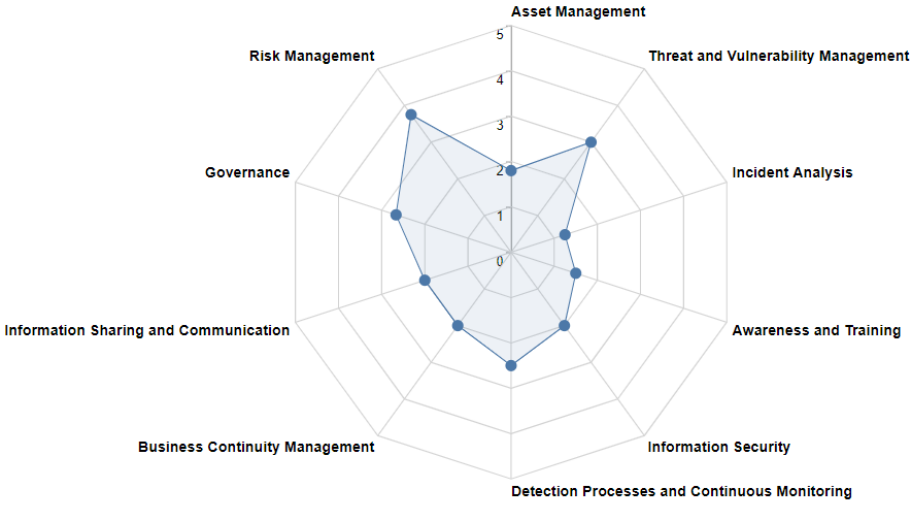

Figure 5.6 Domain-level overview of a mold manufacturer II in the Basque Country

Table 5.7 Summary of evidences and identified actions per domain in case study 6

Domain	Implementation State	Summary of Evidences	Identified Actions
Governance	2.67	The company follows a strategy that defines requirements in the form of risk tolerances for their assets according to their needs and priorities. They know of the GDPR as the only applicable regulation and they have adapted to comply with it and actively make an effort to comply with it fully.	The company has decided to improve this domain by adding a response and recovery component to their strategy. They want to improve in this area to be more resilient. To do this, they will set resilience objectives for their critical assets and try to comply with RTOs and RPOs.
Risk Management	3.75	The company is in a digitalization process with their mind in the risks introduced with the new digitalized business processes. Thus, they are systematically analyzing the risks, their impacts and probability to each of the digitalization they make. The company tries to mitigate any risk that would have a critical impact in the company.	Since this is one of the most advanced domains in their evaluation, the company has decided to prioritize others.
Asset Management	1.80	The company has an inventory of assets that is regularly updated by the IT department. This inventory is done manually. The configuration of systems is standardized with a basic configuration but there is no change control or traceability to determine the current state of the configuration of each system. Maintenance is mainly corrective and their dependency management is based only on their current knowledge and intuition.	The company has decided to start having more control over the configurations of their systems and the interdependencies between them. They have also thought it would be helpful to do preventive maintenance on them to help with configuration control and anticipate problems before they occur.
Threat and Vulnerability Management	3.00	The company has an updated list of threats and vulnerabilities that they found by hiring an external company. In this analysis they found 69 critical vulnerabilities and 13 high vulnerabilities. They have tried to mitigate vulnerabilities these high and critical vulnerabilities.	Since this is one of the most advanced domains in their evaluation, the company has decided to prioritize others.
Incident Analysis	1.25	Since the company has not had major incidents they have not focused on making systematic procedures in this regard. However, they have analyzed the damages done by previous small incidents (spear phishing attempts) to try to add more countermeasures and awareness to the personnel.	Since they have no experience in this area, the company has decided to improve this domain in future iterations.

Awareness and Training	1.50	The company is starting to define training and awareness plans and is also planning on starting an awareness campaign with the help of their cybersecurity provider. However, at the moment, they don't have technical training in cybersecurity.	The company is in the process of defining general cybersecurity training plans for the personnel, especially emphasizing their awareness.
Information Security	2.00	The company has very basic protections such as access control and antiviruses. However, they have an automatic back-up system that uploads a backup daily to the cloud.	The company is considering upgrading their protection measures by improving their network segmentation.
Detection Processes and Continuous Monitoring	2.50	The company monitors the basic indicators for their critical systems. The company also has a very basic detection process in which they have a person responsible of deciding how to solve the incident.	The company wants to expand the monitoring of their assets with better software that lets them monitor more indicators and has automatic alerts for anomalous behaviors.
Business Continuity Management	2.00	The company has untested and undocumented plans that in theory would help them respond and recover. These plans mostly consist on using the clones of the systems they have at the ready.	The company wants to formalize the contingency plans by documenting them and testing them. They would also like to explore the need for plans that deal with incidents that cannot be solved with the existing system clones.
Information Sharing and Communication	2.00	The company has NDA agreements with the cybersecurity providers they have worked with and a documented and well defined contract on the services they outsource, but nothing else.	The company wants to improve this domain by establishing more collaboration relationships to retrieve intelligence of cyber incidents and risks they could be exposed to. They would also like to define a resilience communication plan at least at a basic level.
OVERALL	2.25		

As shown in the evidences of this case study, this company has used the help of cybersecurity providers to improve in many domains, but especially in the risk management and the threat and vulnerability management where they are most advanced. This company's strategy is clearly centered in risk management and the protection against the identified risks.

The company's overall average cyber resilience maturity state suggests that the company has mainly worked on the basic cybersecurity measures. However, unlike the company in the previous case study, the balance and prioritization of the cyber resilience operationalization of this company seems to be slightly incorrect since their Asset Management domain seems to have a below average maturity. This means that although they have implemented protection and mitigation measures, these measures are not the most efficient strategically and that they probably could develop a more informed strategy.

The steps this company identified in order to improve are updating their current inventory to have a better understanding of the assets they currently have, mitigate the critical and high vulnerabilities they have identified in their current systems and improve their business continuity management by formalizing it and testing the plans. These actions are coherent with the implementation order in the CR-OF since the improvement of their asset management can lead to a better risk-based strategy and the mitigation of their current weaknesses can help the company avoid an incident before they set up their strategy. Moreover, improving their business continuity management can help them respond and recover from any incident while they improve in other domains.

5.2 Completeness and Usefulness of the CR-OF

During the case studies, the companies that participated where asked for feedback related to the completeness and usefulness of the presented set of tools (i.e. the CR-OF). All the companies during the case studies gave positive feedback regarding the tools' completeness and usefulness for their needs. Moreover, during the case studies, the companies were able to identify their current maturity in cyber resilience through the self-assessment and used the

reports from the CR-SAT to decide which actions they wanted to improve upon. Then, the companies were able to identify correct actions to implement in order to improve through the progression model's next steps and prioritize them to using the implementation order. Thus, the CR-OF can be considered as a useful tool to reach the end-users (SME cyber resilience operationalization decision-makers) and aid them in the improvement of their cyber resilience operationalization.

However, the CR-OF was not the silver bullet for cyber resilience operationalization and they pointed out several considerations. For instance, they pointed out that this tool needs to be associated to the service of cybersecurity outsourcing companies since in many cases they would not find the tool by themselves or would not prioritize following the process by themselves.

Another possibility suggested by the companies was to automatize the prioritization of the identified actions. The current CR-SAT aids companies in the self-assessment through a questionnaire and identifying actions to improve. However, the prioritization of the identified actions still requires the company to understand their situation and manually compare that situation to the implementation order. This process could be automatized by selecting the objective maturity states in each policy and having a feature that uses the implementation order and a set of known improvement actions to give the users a list of actions in the order they should implement them. This could be achieved by implementing a prioritization algorithm based on the implementation order that uses their selected objectives as an input.

The studied companies' suggestions led to the conclusion that although certain companies might be able to use the CR-OF on their own, there is a need to involve another stakeholder's opinion to evaluate the CR-OF: the cybersecurity providers. Although automation is an option that must be implemented in future research, it could be naïve to implement the results of an automatic tool blindly. Therefore, the use of the CR-OF as a service provided by another party was explored in the next section.

On the other hand, interesting conclusions were drawn from these case studies. Among those conclusions, it was apparent that the companies who relied more in cybersecurity providers had better cyber resilience maturity overall. The same happened for those who were under strict regulation and companies who had suffered cyber incidents in the past. These contextual factors seemed to be drivers in the cyber resilience operationalization of these SMEs.

Moreover, companies with a high emphasis on outsourcing had on average a lower maturity in awareness and training. This result implies that companies are substituting getting internal knowledge in cybersecurity with their cybersecurity providers'. This observation could be further studied and requires analysis because, in the long-term, the lack of internal cyber resilience knowledge could hinder the companies cyber resilience operationalization in the higher maturity levels.

Furthermore, companies with a higher maturity level overall were observed to have a more balanced maturity amongst each of the domains. In other words, companies with a lower maturity overall had prioritized certain domains too much over others. This is consistent with other findings in which defining a cyber resilience investment strategy was found to be more effective when diversifying the investment in different domains in a dynamic manner [136].

Finally, although not with a representative sample, there seems to be an overall advantage in the average maturity level of companies in developed countries such as Spain and the USA in terms of cyber resilience.

5.3 The CR-OF as a Service

As mentioned before, cybersecurity providers seem to play an important role in the operationalization of cyber resilience. Moreover, among the studied companies' suggestions and ideas there seems to be a need for these providers to aid companies in following the CR-OF in order to maximize its potential. Thus, in order to explore the possibility of a cybersecurity provider to use the cyber resilience operationalization framework (CR-OF) as part of their services three

interviews with cybersecurity providers were carried out. During these interviews the objectives were explore possible drivers or barriers to the operationalization of cyber resilience in SMEs and to find out whether it would be of interest to a cybersecurity provider to use the CR-OF with their clients.

Thus, during these interviews, the cybersecurity providers were first asked about the drivers and barriers they saw in the cyber resilience operationalization in SMEs. Then, they were introduced to the CR-OF and the continuous improvement process it encompasses. Finally, they were asked whether they found that the tools in the CR-OF could be useful to them, if yes, they were asked to specify why and how, else they were asked why.

The three interviewed cybersecurity providers identified in a very clear way the drivers and barriers to cyber resilience operationalization in SMEs. Regarding the drivers the three of them agreed that having incidents and having strict laws where the most powerful drivers for cyber resilience operationalization. This introduces a possible new stakeholder into the cyber resilience operationalization in companies: governments and lawmakers. However, this was not explored during this thesis.

Some of the cybersecurity providers also agreed that the supply chain can also be a driver for cyber resilience operationalization since SMEs can be part of the supply chain of a big company, and sometimes these bigger companies require strong cyber resilience operationalization from their suppliers. For instance, they claimed that certain companies might ask their supplier to be certified by a standard or framework in cybersecurity in order to have a secure supply chain. This also led the experts to point out that following frameworks or standards and having support from cybersecurity providers or similar partners could also work as a driver to the cyber resilience operationalization in SMEs. As shown in previous sections of this chapter, this research can attest for most of the drivers mentioned by the cybersecurity providers since these drivers could be observed in the companies that participated in the case studies and did better.

On the other hand, regarding the barriers, the three cybersecurity providers only agreed unanimously to one: a lack of awareness. According to them this is the root of all barriers towards cyber resilience operationalization. This can be

confirmed when other barriers are mentioned: not being able to see the return over investment (ROI) of investing in cybersecurity or considering it as a cost and not an investment. Another commonly mentioned barrier would be that the company has not suffered an incident providing them with a false sense of security. Finally, the other barrier was that companies do not see the value in cybersecurity because it is completely estranged from their normal activity or business.

Understanding the drivers and barriers cybersecurity providers identified in cyber resilience operationalization was useful to understand the possible stakeholders involved in the cyber resilience operationalization and gives interesting insights into the value they could see in the tools presented in the CR-OF. For instance, the barriers mentioned by the cybersecurity providers, related to the lack of knowledge and awareness of SMEs regarding cyber resilience confirms the problem that this thesis aims to solve. However, to ascertain whether they find the CR-OF useful as a possible service to add to their current portfolio they were directly asked about the value they could see as cybersecurity providers to a set of tools such as the CR-OF.

In this regard, the three cybersecurity providers had positive feedback and interest in implementing the CR-OF into their portfolios. However, they all had different ideas on how to implement this into their services. One of the cybersecurity providers thought it would be a nice introductory tool for companies to get interested in more services. The reasoning behind this thought was that companies could self-assess and decide action plans that they might need help implementing through solutions that the provider usually has available whether it be technical solutions or consulting projects.

Another cybersecurity provider had a very similar thought process but thought that the CR-OF itself could be the first product. The reasoning behind this is that for a small subscription price companies could have access to the CR-SAT where they could use it as many times as they wanted. If the company subscribed to the service needed more assistance with a certain implementation they were already working with a cybersecurity provider who could list the services related to each policy of the conceptual framework (CR-CF) that the

company wanted to improve upon. Thus, this way, the cybersecurity provider would have a fidelity tool that also added value to the companies who used it.

The final opinion on the matter was that it would be a great tool to complement their current service portfolio since it goes beyond the competitors by offering a resilience point of view. This cybersecurity provider considered that the market was very saturated with technical solutions that solved cybersecurity problems and that many cybersecurity providers were getting too comfortable as software sellers. However, the interesting part, in his opinion, was that the tool had a more holistic view but also had specific parts regarding the response and recovery. In a sense, this cybersecurity provider believed that the CR-OF could help the cybersecurity providers give a guidance service that other providers are lacking nowadays. This provider even argued that even though most companies knew they had to back up their information and systems, most of them did not know if they could restore a backup if a system was compromised. Adding this to the services could thus be interesting to differentiate from the competitors because of a more guided service and because it would help companies realize how important it is to be prepared to respond and recover in case of an incident.

6

6 Conclusions, Limitations and Future Research

This chapter presents a summary of the outcomes and main conclusions obtained within this research. Moreover, it presents the main limitations of the Cyber resilience operationalization framework (CR-OF) for SMEs. Finally, it proposes the future research lines to address the existing limitations and to increase the scope and benefits of the current version of the CR-OF.

6.1 Conclusions

Cyber resilience is an innovative change of perspective from traditional cybersecurity that promises to make companies "safe-to-fail" systems that are prepared to face cyber incidents and maintain their operations as much as possible. However, cyber resilience is difficult to operationalize because of its holistic, multidimensional and multidisciplinary nature. In this sense, this study aimed to develop a cyber resilience operationalization framework (CR-OF) with a set of tools to aid SMEs in their cyber resilience building process. Thus, the CR-OF is composed of:

1. A cyber resilience conceptual framework (CR-CF) for SMEs to define and enumerate the essential domains and policies required to operationalize cyber resilience in SMEs.
2. An implementation order to outline a general strategy to prioritize the policies for an effective cyber resilience operationalization.
3. A progression model to determine the natural progressions and progression types for the essential cyber resilience policies.
4. A self-assessment and strategic planning tool (CR-SAT) to allow SMEs assess their cyber resilience operationalization and strategize their cyber resilience operationalization through the implementation and evolution of the different policies.
5. A cyber resilience cyber range $(CR)^2$ to increase the awareness of decision makers about the importance of cyber resilience operationalization and the consequences of their investments (or lack thereof).

Table 6.1 shows how these results that compose the CR-OF contribute to the Research Questions and Research Objectives of this thesis.

Table 6.1 Summary of results and contributions to Research Questions and Research Objectives

	Conceptual Framework (CR-CF)	Implementation Order	Cyber Resilience Progression Model	Cyber Resilience Cyber Range $(CR)^2$	Self-Assessment Tool (CR-SAT)
RQ1. What are the essential cyber resilience domains and policies for cyber resilience operationalization in SMEs?	X				
RQ2. How should SMEs prioritize cyber resilience policies for an effective operationalization?		X	X	X	
RQ3. What are the natural progressions and progression types of cyber resilience policies?			X		X
RQ4. How to increase the cyber resilience operationalization decision-makers' awareness?				X	X
Objective 1: Define and enumerate the essential domains and policies required to operationalize cyber resilience in SMEs	X				
Objective 2: Outline a general strategy to prioritize the domains and policies for an effective cyber resilience operationalization.		X			
Objective 3: Determine realistic progressions over time for the essential cyber resilience policies			X		
Objective 4: Develop management tools to: let SMEs self-assess, aid them in the prioritization and strategic planning, and increase the awareness of decision makers				X	X

Moreover, this set of results composing the CR-OF allow SMEs to start their cyber resilience operationalization in a continuous improvement cycle by following the guidelines established in them. Through these results SMEs can also be able to learn the reasons behind these guidelines and operationalize their cyber resilience in a more informed manner and in accordance with their current needs and circumstances.

In this sense, the CR-OF contributes to the current literature since it is the only approach that fulfills the desirable characteristics for SMEs. These characteristics are:

- The specific focus on SMEs as a target **Audience (A)**,
- The means for SMEs to be able to **Self-Assess (SA)** their current situation,
- The means for SMEs to be able to determine the natural next steps through some description of the **Policies' Maturity Evolution (PME).**
- The means for SMEs to be able to **Prioritize (P)** when to implement policies once they decide which ones they wish to implement.

Table 6.2 presents the summary of the current literature and how the CR-OF contributes to it by fulfilling these characteristics.

Table 6.2 Summary of the current literature and CR-OF contribution

Document	A	SA	PME	P
OCTAVE Allegro [101]	Companies	No	No	Yes
IEC 62443 [95]	Companies	No	No	No
COBIT 5 [102]	Companies	No	Yes	No
CR-AF [103]	Banks	No	No	No
Cyber Resiliency Metrics [39]	Companies	No	No	No
Resilience Metrics for Cyber Systems [43]	Federal agencies and Companies	No	No	No
ISO 27001:2013 [87]	Companies	No	No	No
NIST SP 800-53 Rev. 4 [48]	Companies	No	No	No
C2M2 [47]	Companies	Yes	Yes	No
ISO/IEC 15408:2009 [141]	Companies	Yes	No	No
Cyber Resilience Review (CRR) [88]	Companies	Yes	Yes	No
A Framework for Assessing Cyber Resilience [44]	Companies	No	No	No
CERT Resilience Management Model (RMM), Version 1.2 [142]	Companies	No	No	No
How to Steer Cyber Security with Only One KPI: The Cyber Risk Resilience [85]	Companies	No	No	No

Document	A	SA	PME	P
Advancing Cyber Resilience: Principles and Tools for Boards [64]	Companies	No	No	No
NIST CSF [41]	Federal agencies and companies	No	No	No
CIS Controls V7.1 [42]	Companies	No	No	No
BC2M2 [94]	Companies	Yes	Yes	No
Indicadores para la mejora de la ciber resiliencia] [37]	Critical Infrastructures	Yes	Yes	No
AVARCIBER [143]	Companies	Yes	No	No
Lego Methodology Approach for Common Criteria Certification of IoT Telemetry [144]	Companies	Yes	No	No
Assessing information security risks in the cloud: A case study of Australian local government authorities [145]	Governments	Yes	No	No
Understanding the management of cyber resilient systems [146]	Companies	No	No	No
Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS [147]	Companies	No	No	No
Designing Recommendations and Road Map of Governance for Quality Management System of Online SKCK Based on Information Security Using ISO 9001: 2015 and ISO 27001: 2013 (Case Study: Ditintelkam Polda ABC) [148]	Companies	Yes	No	No
Designing an Effective Information Security Policy for Public Organizations: ISO 27001 as a Success Framework [149]	Companies	No	No	No
Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education [150]	Universities	Yes	Yes	No
ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University [151]	Universities	Yes	Yes	No
Improving Cybersafety Maturity of South African Schools [152]	Schools	Yes	No	No
ISM Application Tool [153]	SMEs	Yes	No	No
Math approach of implementing ISO 27001 [154]	Companies	No	No	No
Implementation of Information Security System in Service and Trade [155]	Companies	No	No	No
Cyber Security Defence Policies: A Proposed Guidelines for Organisations Cyber Security Practices [156]	Companies	No	No	No
ISO 27001 information security management standard's implementation in software development environment: a case study [157]	Companies	No	No	No
Independent Co-Assurance using the Safety-Security Assurance Framework (SSAF) [158]	Companies	No	No	No
Analysis of Appropriate Standards to solve Cybersecurity problems in Public Organizations [159]	Public Companies	No	No	No
Guía / Framework para la definición de la función de seguridad [160]	Companies	No	No	No
The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda [161]	Companies	No	No	No
Security Standard Compliance Verification in System of Systems [162]	Companies	Yes	No	No

Document	A	SA	PME	P
Aligning with cybersecurity framework by modelling OT security [163]	Companies	No	No	No
Ensuring information security in public organizations in the republic of Moldova through the ISO 27001 standard [164]	Public Companies	No	No	No
CR-OF	SMEs	Yes	Yes	Yes

6.2 Limitations

Although the tools presented in this study are useful for companies starting their cyber resilience operationalization, they are limited in various ways. In this sense, the main limitations are:

- The set of tools presented in this study are meant to aid companies starting their cyber resilience operationalization and thus exclude nuances that other documents include that might be important for more mature companies. Thus, this study is limited to SMEs and companies starting their cyber resilience operationalization and more mature companies who try to use it might require additional information for a more advanced cyber resilience operationalization.
- Most of the conclusions are drawn from experts' backgrounds and experiences, but most of the experts (though not all of them) are from the Basque Country. Their regional background might have influenced the results and thus these results must be contrasted in other regions to corroborate applicability in those regions.
- The time and resources used to operationalize cyber resilience with the aid of these tools has not been measured and quantitative analysis considering and optimizing these parameters are still lacking.

6.3 Future Research

This study presents tools that view cyber resilience from a top-down approach and thus set the base towards a plethora of different, smaller roads that have not been explored in detail. In this sense, the bottom-up approach, or the study of specific policies and their effective implementation, nuances and particularities should still be studied through future research.

On the other hand, future research should also comprise and complement the limitations of this study. Thus, to reaffirm the validity of these results and

improve cyber resilience operationalization in companies, future research should:

- Contrast the results by developing similar studies with experts from different regions to be able to generalize them into other countries and cultures.
- Design and develop quantitative analyses to explore, confirm and potentially optimize these results with quantitative data. This would complement and improve the qualitative approach that prevails in this study.
- Explore the cyber resilience operationalization of more mature companies to understand the different approaches (if they exist) that these tools require in order to aid companies in a more advanced maturity or that are further into the process of cyber resilience operationalization.
- Extend the evaluation of the CR-OF with a new version of the tools in which the CR-SAT automatically suggests the actions and prioritization the company should follow in order to improve their cyber resilience.
- Explore and study the different stakeholders in cyber resilience operationalization to understand and overcome possible conflicts of interest and take advantage of synergies between them.

7 References

[1] World Economic Forum, "The global risks report 2018, 13th edition," Geneva, Switzerland, 2018, [Online]. Available: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.

[2] Allianz Global Corporate & Speciality, "Allianz Risk Barometer: Top Business Risks for 2019," Munich, Germany, 2019, [Online]. Available: http://www.agcs.allianz.com/insights/white-papers-and-case-studies/risk-barometer-2015/.

[3] Symantec, "Internet Security Threat Report," CA, USA, 2017, [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

[4] ENISA, "ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends About ENISA," Athens, Greece, 2018, [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[5] C. Alcaraz, R. Rom, and J. E. Rubio, "Estado y Evolucion de la Deteccion de Intrusiones en los Sistemas Industriales," 2017, no. Jnic, pp. 1–20.

[6] F. Björk, M. Henkel, J. Stirna, and J. Zdravkovic, "Cyber Resilience –

Fundamentals for a Definition," *Adv. Intell. Syst. Comput.*, vol. 353, no. January, pp. III–IV, 2015, doi: 10.1007/978-3-319-16486-1.

[7] K. Zetter, *Countdown to Zero Day*, 1st ed. New York: Crown Publishers, 2014.

[8] Norton Team, "The 8 Most Famous Computer Viruses of All Time," *Norton UK Blog*, 2016. [Online]. Available: https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html. [Accessed: 27-Jun-2018].

[9] K. Okereafor and R. Djehaiche, "A Review of Application Challenges of Digital Forensics," *Int. J. Simul. Syst. Sci. Technol.*, vol. 21, no. 2, pp. 31–35, 2020.

[10] BBC Mundo, "Ciberataque masivo: ¿quiénes fueron los países e instituciones más afectados por el virus WannaCry?," *BBC Mundo*, 15-May-2017.

[11] ABC, "Un ataque informático amenaza al portal de citas extramatrimoniales Ashley Madison," *ABC Tecnología*, 19-Aug-2015.

[12] M. Valle, "Estados Unidos se sincera: más de 21 millones de personas afectadas en el último ciberataque," *Globb Security*, 2015. [Online]. Available: http://globbsecurity.com/opm-ciberataque-21-millones-35146/. [Accessed: 10-Apr-2018].

[13] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *WIRED*, p. 21, Jul-2015.

[14] New Net Technologies, "EternalBlue Exploit Used in WannaCry Attack," *NNT*, 2018. [Online]. Available: https://www.newnettechnologies.com/eternalblue-exploit-used-in-wannacry-ransomware-attack.html. [Accessed: 28-Jun-2018].

[15] R. Langde, "WannaCry Ransomware: A Detailed Analysis of the Attack," *TechPerspective*, 2017. [Online]. Available: https://techspective.net/2017/09/26/wannacry-ransomware-detailed-analysis-attack/. [Accessed: 28-Jun-2018].

[16] Kapersky, "What is WannaCry ransomware?," *Kapersky*, 2021. [Online]. Available: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. [Accessed: 03-Nov-2019].

[17] T. Lee, "The WannaCry ransomware attack was temporarily halted. But it's not over yet.," *Vox*, 2017. [Online]. Available: https://www.vox.com/new-money/2017/5/15/15641196/wannacry-ransomware-windows-xp. [Accessed: 28-Jun-2018].

[18] IT Governance, "An introduction to implementing cyber resilience," 2018.

[19] ENISA, "Information security and privacy standards for SMEs," Athens, Greece, 2015, [Online]. Available: https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport.

[20] J. Lewis, "Economic Impact of Cybercrime—No Slowing Down Report," 2018, [Online]. Available: https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf.

[21] S. McManus, E. Seville, J. Vargo, and D. Brunsdon, "Facilitated Process for Improving Organizational Resilience," *Nat. Hazards Rev.*, vol. 9, no. 2, pp. 81–90, 2008, doi: 10.1061/(ASCE)1527-6988(2008)9:2(81).

[22] D. Tofan, T. Nikolakopoulos, and E. Darra, "The Cost of Incidents Affecting CIIs: Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII)," ENISA, Athens, Greece, 2016, [Online]. Available: https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/.

[23] World Economic Forum, "The Global Risks Report 2020," Geneva, Switzerland, 2020, [Online]. Available: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

[24] M. Damiano, "VIPRE Announces Launch of VIPRE Endpoint Security - Cloud Edition | Business Wire," *Business Wire*, 2017. [Online]. Available: https://www.businesswire.com/news/home/20171002005176/en. [Accessed: 28-Oct-2019].

[25] Federation of Small Businesses, "Cyber Resilience : How To Protect Small Firms in the Digital Economy," Blackpool, England, 2016, [Online]. Available: http://www.fsb.org.uk/docs/default-source/fsb-org-uk/fsb-cyber-resilience-report-2016.pdf?sfvrsn=0.

[26] P. Millaire, A. Sathe, and P. Thielen, "What All Cyber Criminals Know: Small & Midsize Businesses With Little or No Cybersecurity Are Ideal Targets," NJ, USA, 2017, [Online]. Available: https://www.chubb.com/us-en/_assets/doc/17010201-cyber-for-small_midsize-businesses-10.17.pdf.

[27] P. A. H. Williams and R. J. Manheke, "Small Business - A Cyber Resilience Vulnerability," in *International Cyber Resilience Conference*, 2010, no. August, pp. 112–117.

[28] M. Aminul Islam, M. Aktaruzzaman Khan, A. Z. M. Obaidullah, and M. Syed Alam, "Effect of Entrepreneur and Firm Characteristics on the Business Success of Small and Medium Enterprises (SMEs) in

Bangladesh," *Int. J. Bus. Manag.*, vol. 6, no. 3, 2011, doi: 10.5539/ijbm.v6n3p289.

[29] T. Mazzarol, T. Volery, N. Doss, and V. Thein, "Factors influencing small business start-ups," *Int. J. Entrep. Behav. Res.*, vol. 5, no. 2, pp. 48–63, 1999, doi: 10.1108/13552559910274499.

[30] K. E. Neupert, C. C. Baughn, and T. T. Lam Dao, "SME exporting challenges in transitional and developed economies," *J. Small Bus. Enterp. Dev.*, vol. 13, no. 4, pp. 535–545, 2006, doi: 10.1108/14626000610705732.

[31] T. Huelsman and S. Peasley, "Cyber risk in advanced manufacturing," VA, USA, 2016, [Online]. Available: https://www.nist.gov/sites/default/files/documents/2016/12/28/cyberrisk_manu_fullstudy_landscape_brochure_lpxcic07_06_17_7101_finalfor.pdf.

[32] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decis. Support Syst.*, vol. 86, pp. 13–23, 2016, doi: 10.1016/j.dss.2016.02.012.

[33] T. I. Vaaland and M. Heide, "Can the SME survive the supply chain challenges?," *Supply Chain Manag.*, vol. 12, no. 1, pp. 20–31, 2007, doi: 10.1108/13598540710724374.

[34] C. Crane, "15 Small Business Cyber Security Statistics That You Need to Know - Hashed Out by The SSL Store™," 2019. [Online]. Available: https://www.thesslstore.com/blog/15-small-business-cyber-security-statistics-that-you-need-to-know/. [Accessed: 28-Oct-2019].

[35] P. Binwal, "Creating a Cybersecurity Governance Framework: The Necessity of Time," *Security Intelligence*, 2015. [Online]. Available: https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time/. [Accessed: 17-Dec-2019].

[36] H. Goldman, R. McQuaid, and J. Picciotto, "Cyber resilience for mission assurance," in *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, 2011, no. April, pp. 236–241, doi: 10.1109/THS.2011.6107877.

[37] INCIBE, "Indicadores para Mejora de la Ciberresiliencia (IMC)," Madrid, Spain, 2019, [Online]. Available: https://www.incibe-cert.es/guias-y-estudios/guias/imc-indicadores-mejora-ciberresiliencia.

[38] S. A. Deutscher, W. Bohmayr, and A. Asen, "Building a Cyberresilient Organization," Boston, MA, USA, 2017, [Online]. Available: https://image-src.bcg.com/Images/BCG-Building-a-Cyberresilient-Organization-Jan-2017_tcm26-186244.pdf.

[39] MITRE, "Cyber Resiliency Metrics," VA, USA, 2012, [Online]. Available:

https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf.

[40] G. Sharkov, "From cybersecurity to collaborative resiliency," in *SafeConfig 2016 - Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, co-located with CCS 2016*, 2016, pp. 3–9, doi: 10.1145/2994475.2994484.

[41] NIST, "Framework for Improving Critical Infrastructure Cybersecurity v 1.1," Gaithersburg, MD, USA, 2018, [Online]. Available: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[42] Center for Internet Security (CIS), "CIS Controls V 7.1," NY, USA, 2019, [Online]. Available: www.cisecurity.org/controls/.

[43] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," *Environ. Syst. Decis.*, vol. 33, no. 4, pp. 471–476, 2013, doi: 10.1007/s10669-013-9485-y.

[44] World Economic Forum, "A framework for assessing cyber resilience," Geneva, Switzerland, 2016, [Online]. Available: http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf.

[45] L. F. Cranor, "A Framework for Reasoning About the Human in the Loop," in *Proceedings of the 1st Conference on Usability, Psychology, and Security*, 2008, pp. 1:1--1:15, doi: 10.5555/1387649.

[46] B. Schneier, "The future of incident response," *IEEE Security and Privacy*, vol. 12, no. 5. pp. 96–97, 2014, doi: 10.1109/MSP.2014.102.

[47] Department of Energy (DOE), "Cybersecurity Capability Maturity Model (C2M2)," Washington DC, USA, 2014, [Online]. Available: https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program.

[48] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev. 4)," Gaithersburg, MD, USA, 2013, [Online]. Available: http://csrc.nist.gov/%0Ahttps://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-4/archive/2013-04-30/documents/sp800-53-rev4-ipd.pdf.

[49] G. Cybenko, "Quantifying and measuring cyber resiliency," in *Proc. SPIE 9825, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement Applications XV*, 2016, vol. 9825, p. 98250R, doi: 10.1117/12.2230586.

[50] L. Pesante, "Introduction to Information Security," *Us Cert*, no. January, pp. 1–3, 2008.

[51] International Organization for Standarization (ISO), "Information technology — Security techniques — Code of practice for information security management Technologies (ISO 27002:2005)," Geneva, Switzerland, 2005, [Online]. Available: http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf.

[52] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[53] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cyber-security," *Technol. Innov. Manag. Rev.*, no. October, pp. 13–21, 2014, doi: 10.22215/timreview/1107.

[54] R. Kemmerer, "Cybersecurity," in *25th International Conference on Software Engineering (ICSE'03)*, 2003, no. 25, pp. 705–715, doi: 10.1017/CBO9781107415324.004.

[55] J. a Lewis, "Cybersecurity and Critical Infrastructure Protection," *Cent. Strateg. Int. Stud. (...*, no. January, pp. 1–12, 2006, doi: 10.1016/B978-0-12-415803-0.00008-8.

[56] E. Amoroso, *Cyber Security*. New Jersey: Silicon Press, 2006.

[57] International Telecommunication Union, "Overview of Cybersecurity," 2009, [Online]. Available: http://www.itu.int/rec/T-REC-X.1205-200804-I/en.

[58] CNSS, "National Information Assurance (IA) glossary," 2010, [Online]. Available: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

[59] Public Safety Canada, "Emergency Management Vocabulary," 2012, [Online]. Available: http://publications.gc.ca/collections/collection_2012/tpsgc-pwgsc/S52-2-281-2012.pdf.

[60] C. Canongia and R. Mandarino Jr., *Cybersecurity: The new challenge of the information society*. 2011.

[61] Oxford University Press, "Oxford Online Dictionary," *Oxford University Press*, 2014. [Online]. Available: https://en.oxforddictionaries.com/definition/Cybersecurity.

[62] NICCS, "Explore Terms: A Glossary of Common Cybersecurity Terminology," *National Initiative for Cybersecurity Carreers and Studies*, 2014. [Online]. Available: https://niccs.us-cert.gov/glossary. [Accessed: 21-

Mar-2018].

[63] European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," 2013.

[64] World Economic Forum, "Advancing Cyber Resilience - Principles and Tools for Boards," Geneva, Switzerland, 2017, [Online]. Available: http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

[65] G. Howser and B. McMillin, "Using Information-Flow Methods to Analyze the Security of Cyber-Physical Systems," *Computer (Long. Beach. Calif).*, vol. 50, no. 4, pp. 17–26, 2017, doi: 10.1109/MC.2017.112.

[66] N. R. Sikula, J. W. Mancillas, I. Linkov, and J. A. McDonagh, "Risk management is not enough: a conceptual model for resilience and adaptation-based vulnerability assessments," *Environ. Syst. Decis.*, vol. 35, no. 2, pp. 219–228, 2015, doi: 10.1007/s10669-015-9552-7.

[67] DHS, "Resilience," *Department of Homeland Security*, 2018. [Online]. Available: https://www.dhs.gov/topic/resilience. [Accessed: 06-Feb-2018].

[68] European Commission, "Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE," 2017, [Online]. Available: https://ec.europa.eu/transparency/regdoc/rep/10101/2017/ES/JOIN-2017-450-F1-ES-MAIN-PART-1.PDF.

[69] UNISDR, "'Terminology: basic terms of disaster risk reduction,'" *United Nations International Strategy for Disaster Reduction – UN-ISDR.*, vol. 2015, no. July 1. 2007.

[70] UNISDR, "Sendai Framework for Disaster Risk Reduction 2015-2030," 2015, [Online]. Available: http://www.unisdr.org/files/43291_sendaiframeworkfordrren.pdf. [Accessed: 12-Jan-2016].

[71] UNISDR, "Hyogo framework for action 2005-2015: building the resilience of nations and communities to disasters," 2005.

[72] M. Bruneau *et al.*, "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthq. Spectra*, vol. 19, no. 4, pp. 733–752, 2003.

[73] L. Labaka, J. Hernantes, E. Rich, and J. M. Sarriegi, "Resilience Building Policies and their Influence in Crisis Prevention, Absorption and Recovery," *J. Homel. Secur. Emerg. Manag.*, vol. 10, no. 1, pp. 289–317, 2013.

[74] T. Aven, "How some types of risk assessments can support resilience

analysis and management," *Reliab. Eng. Syst. Saf.*, vol. 167, pp. 536–543, Nov. 2017, doi: 10.1016/J.RESS.2017.07.005.

[75] T. Morbin, "Risk management to strategic resilience: The evolution of cyber-security," *SC Media UK*, 2017. [Online]. Available: https://www.scmagazineuk.com/risk-management-to-strategic-resilience-the-evolution-of-cyber-security/article/687616/. [Accessed: 02-Jul-2018].

[76] L. Borsa, P. Frank, and H. Doran, "How can resilience prepare companies for environmental and social change?," *Resil. A J. Strateg. risk*, pp. 1–8, 2014.

[77] D. W. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It*, vol. 53, no. 9. 2009.

[78] I. Linkov *et al.*, "Measurable resilience for actionable policy," *Environ. Sci. Technol.*, vol. 47, no. 18, pp. 10108–10110, 2013, doi: 10.1021/es403443n.

[79] J. Hernantes, E. Rich, A. Laugé, L. Labaka, and J. M. Sarriegi, "Learning before the storm: Modeling multiple stakeholder activities in support of crisis management, a practical case," *Technol. Forecast. Soc. Change*, vol. 80, no. 9, 2013, doi: 10.1016/j.techfore.2013.01.002.

[80] O. Weber *et al.*, "FINDINGS FROM THE 2016 SUSTAINABILITY GLOBAL EXECUTIVE STUDY AND RESEARCH PROJECT Investing For a Sustainable Future RESEARCH REPORT In collaboration with," *J. Sustain. Financ. Invest.*, vol. 1, no. 3, pp. 81–87, 2014, doi: 10.1017/CBO9781107415324.004.

[81] T. Aoyama, H. Naruoka, I. Koshijima, W. Machii, and K. Seki, "Studying resilient cyber incident management from large-scale cyber security training," in *2015 10th Asian Control Conference: Emerging Control Techniques for a Sustainable World, ASCC 2015*, 2015, doi: 10.1109/ASCC.2015.7244713.

[82] B. Dupont, "The cyber-resilience of financial institutions: Significance and applicability," *J. Cybersecurity*, vol. 5, no. 1, pp. 1–17, 2019, doi: 10.1093/cybsec/tyz013.

[83] E. Hollnagel, D. Woods, and N. Leveson, *Resilience Engineering: Concepts and Precepts*, 1st ed. Hampshire, England: Ashgate Pub Co, 2006.

[84] E. Kádena, "Security of mobile devices in the view of Swiss Cheese Model," in *Kiberbiztonság/Cybersecurity*, Z. Rajnai, Ed. Budapest: Doctoral School of Security Sciences, 2019, pp. 176–183.

[85] J. Nys, "How to Steer Cyber Security with Only One KPI: The Cyber Risk Resilience," *RSA Conference*. San Francisco, CA, USA, pp. 1–42, 2016.

[86] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "The impact of

information sharing on cybersecurity underinvestment: A real options perspective," *J. Account. Public Policy*, vol. 34, no. 5, pp. 509–519, 2015, doi: 10.1016/j.jaccpubpol.2015.05.001.

[87] International Organization for Standarization (ISO), "ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements," Geneva, Switzerland, 2013, [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

[88] Carnegie Mellon University, "Cyber Resilience Review (CRR)," *Department of Homeland Security*, 2016. [Online]. Available: https://www.us-cert.gov/ccubedvp/assessments. [Accessed: 06-Feb-2018].

[89] M. Vega-Barbas, V. A. Villagrá, F. Monje, R. Riesco, X. Larriva-Novo, and J. Berrocal, "Ontology-based system for dynamic risk management in administrative domains," *Appl. Sci.*, vol. 9, no. 21, 2019, doi: 10.3390/app9214547.

[90] M. Malatji, S. Von Solms, and A. Marnewick, "Socio-technical systems cybersecurity framework," *Inf. Comput. Secur.*, vol. 27, no. 2, pp. 233–272, 2019, doi: 10.1108/ICS-03-2018-0031.

[91] J. F. Carias, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, "Systematic Approach to Cyber Resilience Operationalization in SMEs," *IEEE Access*, vol. 8, pp. 174200–174221, 2020, doi: 10.1109/ACCESS.2020.3026063.

[92] M. Benz and D. Chatterjee, "Calculated risk? A cybersecurity evaluation tool for SMEs," *Bus. Horiz.*, vol. 63, no. 4, pp. 531–540, 2020, doi: 10.1016/j.bushor.2020.03.010.

[93] D. A. Sepúlveda Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," *Comput. Secur.*, vol. 97, 2020, doi: 10.1016/j.cose.2020.101996.

[94] Pacific Northwest National Laboratory, "Buildings Cybersecurity Capability Maturity Model," Washington DC, USA, 2019, [Online]. Available: https://bc2m2.pnnl.gov/. [Accessed: 16-Oct-2019].

[95] International Standards on Auditing (ISA), "ANSI/ISA–62443-2-1 (99.02.01) Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program." ISA, Research Triangle Park, NC, USA, pp. 1–170, 2009.

[96] S. N. G. Gourisetti, S. Mix, M. Mylrea, C. Bonebrake, and M. Touhiduzzaman, "Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2)," in *Proceedings of the Northwest*

Cybersecurity Symposium on - NCS '19, 2019, pp. 1–9, doi: 10.1145/3332448.3332461.

[97] E. Baikloy, P. Praneetpolgrang, and N. Jirawichitchai, "Development of cyber resilient capability maturity model for cloud computing services," *TEM J.*, vol. 9, no. 3, pp. 915–923, 2020, doi: 10.18421/TEM93-11.

[98] R. Caralli, M. Knight, and A. Montgomery, "Maturity models 101: a primer for applying maturity models to smart grid security, resilience, and interoperability," 2012, [Online]. Available: http://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_58920.pdf.

[99] A. Carneiro, "Maturity and Metrics in Health Organizations Information Systems," in *Handbook of Research on ICTs and Management Systems for Improving Efficiency in Healthcare and Social Care*, Lisbon, Portugal: IGI Global, 2013, pp. 937–952.

[100] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Comput. Human Behav.*, vol. 48, pp. 51–61, 2015, doi: 10.1016/j.chb.2015.01.039.

[101] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process," PA, USA, 2007, [Online]. Available: https://kilthub.cmu.edu/articles/journal_contribution/Introducing_OCTAVE_Allegro_Improving_the_Information_Security_Risk_Assessment_Process/6574790.

[102] ISACA, "A Business Framework for the Governance and Management of Enterprise IT," IL, USA, 2012, [Online]. Available: www.isaca.org.

[103] Hong Kong Monetary Authority, "Cyber Resilience Assessment Framework," Hong Kong, China, 2016, [Online]. Available: https://docplayer.net/storage/82/85773113/1595943763/PcrhUos-qhsdL04obl2tUQ/85773113.pdf.

[104] R. A. Caralli, J. H. Allen, D. W. White, L. R. Young, N. Mehravari, and P. D. Curtis, "CERT Resilience Management Model , Version 1 . 2," Pittsburgh, PA, USA, 2016, [Online]. Available: https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf.

[105] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[106] J. Venable and R. Baskerville, "Eating our own Cooking: Toward a Design Science of Research Methods," *Electron. J. Bus. Res. Methods*, vol. 10, no. 2, pp. 141–153, 2012.

[107] A. Hevner, S. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Q.*, vol. 28, no. 1, p. 75, 2004, doi: 10.2307/25148625.

[108] M. Lind, D. Rudmark, and U. Seigerroth, "Design Science Research for Business Process Design: Organizational Transition at Intersport Sweden," in *IFIP WG 8.2/8.6 International Working Conference*, 2010, pp. 159–176, doi: 10.1007/978-3-642-12113-5_10.

[109] D. Jones and S. Gregor, "The Anatomy of a Design Theory," *J. Assoc. Inf. Syst.*, vol. 8, no. 5, pp. 312–335, May 2007, doi: 10.17705/1jais.00129.

[110] B. G. Glaser and A. L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Reprint. Piscataway, NJ, United States: Transaction Publishers, 2009.

[111] D. J. Roman, M. Osinski, and R. H. Erdmann, "El proceso de construcción de la grounded theory en administración," *Contaduria y Adm.*, vol. 62, no. 3, pp. 985–1000, 2017, doi: 10.1016/j.cya.2016.06.012.

[112] R. Azmi, W. Tibben, and K. T. Win, "Review of cybersecurity frameworks: context and shared concepts," *J. Cyber Policy*, vol. 3, no. 2, pp. 258–283, 2018, doi: 10.1080/23738871.2018.1520271.

[113] G. A. Bowen, "Document analysis as a qualitative research method," *Qual. Res. J.*, vol. 9, no. 2, pp. 27–40, 2009, doi: 10.3316/QRJ0902027.

[114] J. Corbin and A. L. Strauss, *Basics of qualitative research: grounded theory procedures and techniques*, 4th ed. Thousand Oaks, CA, USA: Sage Publications, 2014.

[115] J. Saldaña, *The coding manual for qualitative researchers*, 3rd ed. Thousand Oaks, CA, USA: SAGE Publications, 2015.

[116] B. G. Glaser, *Theoretical sensitivity: advances in the methodology of grounded theory*, 5th ed. Mill Valley, CA, USA: Sociology Press, 1978.

[117] M. Wiesche, M. C. Jurisch, P. W. Yetton, and H. Krcmar, "Grounded Theory Methodology in Information Systems Research," *MIS Q.*, vol. 41, no. 3, pp. 685–701, Mar. 2017, doi: 10.25300/MISQ/2017/41.3.02.

[118] A. L. Strauss, *Qualitative Analysis for Social Scientists*, Reprint. Cambridge, England: Cambridge University Press, 1987.

[119] B. K. Louise and W. Alison, "Collecting data using a semi-structured

interview: a discussion paper," *J. Adv. Nurs.*, vol. 19, no. 2, pp. 328–335, 1994.

[120] E. W. Treece and J. W. Treece Jr, "ELEMENTS OF RESEARCH IN NURSING," *AJN Am. J. Nurs.*, vol. 74, no. 3, p. 567, 1974.

[121] CMMI Product Team, "CMMI® for Development: improving processes for better products," Pittsburgh, PA, USA, 2006.

[122] C. Schmidt, "The Analysis of Semi-structured Interviews," in *A Companion to Qualitative Research*, English., U. Flick, E. von Kardorff, and I. Steinke, Eds. London, UK: SAGE Publications, 2004, pp. 253–258.

[123] M. Łatuszyńska, "System Dynamics Modeling in Behavioral Decision Making," in *Neuroeconomic and Behavioral Aspects of Decision Making*, 2017, pp. 243–253.

[124] J. W. Forrester, "Information Sources for Modeling the National Economy," *J. Am. Stat. Assoc.*, vol. 75, no. 371, pp. 555–566, 1980.

[125] D. N. Ford and J. D. Sterman, "Expert knowledge elicitation to improve formal and mental models," *Syst. Dyn. Rev.*, vol. 14, no. 4, pp. 309–340, 1998, doi: 10.1002/(SICI)1099-1727(199824)14:4<309::AID-SDR154>3.0.CO;2-5.

[126] G. P. Richardson and A. L. Pugh, *Introduction to System Dynamics Modeling*. Pegasus Communications, 1981.

[127] J. Gerring, "What Is a Case Study and What Is It Good for?," *Am. Polit. Sci. Rev.*, vol. 98, no. 2, pp. 341–354, May 2004, doi: 10.1017/S0003055404001182.

[128] R. K. Yin, *Case study research and applications: Design and methods*, 6th ed. Thousand Oaks, CA: SAGE Publications, 2018.

[129] Z. Zainal, "Der Krieg und die Liebe - Untersuchungen zur römischen Venus," *J. Kemanus.*, vol. 5, no. 1, pp. 1–6, 2007.

[130] M. Tickle, D. Adebanjo, and Z. Michaelides, "Developmental approaches to B2B virtual communities," *Technovation*, vol. 31, no. 7, pp. 296–308, 2011, doi: 10.1016/j.technovation.2011.04.002.

[131] N. Kshetri, *The Global Cybercrime Industry*, 1st ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[132] Ponemon Institute, "2011 Cost of Data Breach Study: Australia," MI, USA, 2012, [Online]. Available: https://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-australia-us.pdf.

[133] C. Pham, D. Tang, K. Chinen, and R. Beuran, "CyRIS: A Cyber Range Instantiation System for Facilitating Security Training," in *Proceedings of*

the Seventh Symposium on Information and Communication Technology, 2016, pp. 251–258, doi: 10.1145/3011077.3011087.

[134] W. Braun, "The system archetypes," *System*, vol. 2002, p. 27, 2002.

[135] BCSC, "Basque Cyber Security Center," 2021. [Online]. Available: https://www.basquecybersecurity.eus/en/. [Accessed: 10-Mar-2021].

[136] J. F. Carias *et al.*, "Defining a cyber resilience investment strategy in an industrial internet of things context," *Sensors (Switzerland)*, vol. 19, no. 1, p. 138, Jan. 2019, doi: 10.3390/s19010138.

[137] J. F. Carias, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, "The Order of the Factors DOES Alter the Product: Cyber Resilience Policies' Implementation Order," in *Computational Intelligence in Security for Information Systems Conference (CISIS)*, Burgos, Spain: Springer, 2021, pp. 306–315.

[138] Ziur, "Ziur," 2021. [Online]. Available: https://www.ziur.eus/en/. [Accessed: 10-Mar-2021].

[139] INCIBE, "Instituto Nacional de Ciberseguridad de España," 2021. [Online]. Available: https://www.incibe.es/en. [Accessed: 03-Oct-2021].

[140] BCSC, "White Paper on Cybersecurity in the Basque Country," Alava, Spain, 2021, [Online]. Available: https://www.basquecybersecurity.eus/archivos/202102/bcsc_libro-blanco_ingles_01.pdf.

[141] International Organization for Standarization (ISO), "ISO/IEC 15408:2009 Information technology — Security techniques — Evaluation criteria for IT security." ISO, Geneva, Switzerland, pp. 1–64, 2014.

[142] Software Engineering Institute, "CERT Resilience Management Model (CERT-RMM) Version 1.2," *Carnegie Melon University*, 2016. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084. [Accessed: 25-Jun-2018].

[143] A. M. Rea-Guaman, J. Mejía, T. San Feliu, and J. A. Calvo-Manzano, "AVARCIBER: a framework for assessing cybersecurity risks," *Cluster Comput.*, vol. 23, no. 3, pp. 1827–1843, 2020, doi: 10.1007/s10586-019-03034-9.

[144] G. Suciu, C. Istrate, I. Petre, and A. Scheianu, "Lego Methodology Approach for Common Criteria Certification of IoT Telemetry," in *New Knowledge in Information Systems and Technologies. WorldCIST'19*, vol. 930, A. Rocha, H. Adeli, L. P. Reis, and S. Costanzo, Eds. Cham, Switzerland: Springer, 2019, pp. 165–174.

[145] O. Ali, A. Shrestha, A. Chatfield, and P. Murray, "Assessing information security risks in the cloud: A case study of Australian local government authorities," *Gov. Inf. Q.*, vol. 37, no. 1, p. 101419, 2020, doi: 10.1016/j.giq.2019.101419.

[146] A. Annarelli, F. Nonino, and G. Palombi, "Understanding the management of cyber resilient systems," *Comput. Ind. Eng.*, vol. 149, no. January, p. 106829, 2020, doi: 10.1016/j.cie.2020.106829.

[147] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss," *Int. J. Informatics Vis.*, vol. 4, no. 4, pp. 225–230, 2020, doi: 10.30630/joiv.4.4.482.

[148] P. P. Putra, A. A. Arman, I. J. M. Edward, and W. Shalannanda, "Designing recommendations and road map of governance for quality management system of online SKCK based on information security using ISO 9001: 2015 and ISO 27001: 2013 (Case Study: Ditintelkam Polda ABC)," *Proceeding 14th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2020*, vol. 2013, no. 3, pp. 0–6, 2020, doi: 10.1109/TSSA51342.2020.9310824.

[149] Y. Maleh and M. Belaissaoui, "Designing an Effective Information Security Policy for Public Organizations," no. November, pp. 1176–1193, 2020, doi: 10.4018/978-1-7998-3473-1.ch081.

[150] I. Mantra, A. Abd. Rahman, and H. Saragih, "Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education," *Int. J. Eng. Technol.*, vol. 9, no. 2, p. 429, 2020, doi: 10.14419/ijet.v9i2.30581.

[151] A. Y. Eskaluspita, "ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 879, no. 1, p. 012074, Aug. 2020, doi: 10.1088/1757-899X/879/1/012074.

[152] E. Kritzinger, "Improving cybersafety maturity of South African schools," *Inf.*, vol. 11, no. 10, pp. 1–17, 2020, doi: 10.3390/info11100471.

[153] N. A. Chandra and M. Sadikin, "ISM application tool, a contribution to address the barrier of information security management system implementation," *J. Inf. Commun. Converg. Eng.*, vol. 18, no. 1, pp. 39–48, 2020, doi: 10.6109/jicce.2020.18.1.39.

[154] L. A. Stoica and R. A. Candoi-Savu, "Math approach of implementing ISO 27001," *Proc. Int. Conf. Bus. Excell.*, vol. 14, no. 1, pp. 521–530, 2020, doi: 10.2478/picbe-2020-0049.

[155] A. Nechai, E. Pavlova, T. Batova, and V. Petrov, "Implementation of Information Security System in Service and Trade," *IOP Conf. Ser. Mater. Sci.*

Eng., vol. 940, no. 1, 2020, doi: 10.1088/1757-899X/940/1/012048.

[156] J. O. Oyelami and A. M. Kassim, "Cyber security defence policies: A proposed guidelines for organisations cyber security practices," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 8, pp. 131–138, 2020, doi: 10.14569/IJACSA.2020.0110817.

[157] A. Ojalainen, "Iso 27001 Information Security Management Standard ' S Implementation in Software De- Velopment Environment : a Case Study," University of Jyväskylä, 2020.

[158] N. Johnson, Y. Gheraibia, and T. Kelly, "Independent Co-Assurance using the Safety-Security Assurance Framework (SSAF): A bayesian belief network implementation for IEC 61508 and common criteria," *arXiv*, 2020.

[159] S. M. T. Toapanta, E. Gustavo Salomon Gaibor, and L. E. M. Gallegos, "Analysis of appropriate standards to solve cybersecurity problems in public organizations," *ACM Int. Conf. Proceeding Ser.*, no. June, pp. 14–19, 2020, doi: 10.1145/3404663.3404678.

[160] M. Penilla, "Guía / Framework para la definición de la función de seguridad," San Sebastian, Spain, 2021, [Online]. Available: https://www.ziur.eus/documents/124537/0/Guía-Framework+seguridad_vF+%281%29.pdf/709547bc-cce9-8287-1126-70aa54923509?t=1613472119267.

[161] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *TQM J.*, vol. 33, no. 7, pp. 76–105, 2021, doi: 10.1108/TQM-09-2020-0202.

[162] A. Bicaku, M. Zsilak, P. Theiler, M. Tauber, and J. Delsing, "Security Standard Compliance Verification in System of Systems," *IEEE Syst. J.*, pp. 1–11, 2021, doi: 10.1109/jsyst.2021.3064196.

[163] M. Parekh, K. Waedt, and A. Tellabi, "Aligning with cybersecurity framework by modelling OT security," in *INFORMATIK 2020*, 2021, pp. 311–319, doi: 10.18420/inf2020_29.

[164] A. Alexei, "Ensuring Information Security in Public Organizations in the Republic of Moldova Through the Iso 27001 Standard," *J. Soc. Sci.*, vol. IV(1), 2021, doi: 10.52326/jss.utm.2021.4(1).11.

[165] G. V Glass, P. D. Peckham, and J. R. Sanders, "Consequences of Failure to Meet Assumptions Underlying the Fixed Effects Analyses of Variance and Covariance," *Rev. Educ. Res.*, vol. 42, no. 3, pp. 237–288, Sep. 1972, doi: 10.3102/00346543042003237.

[166] T. Dong, L. Tian, A. Hutson, and C. Xiong, "Parametric and non-parametric confidence intervals of the probability of identifying early disease stage given sensitivity to full disease and specificity with three ordinal diagnostic groups," *Stat. Med.*, vol. 30, no. 30, pp. 3532–3545, Dec. 2011, doi: 10.1002/sim.4401.

[167] L. M. Lix, J. C. Keselman, and H. J. Keselman, "Consequences of Assumption Violations Revisited: A Quantitative Review of Alternatives to the One-Way Analysis of Variance 'F' Test," *Rev. Educ. Res.*, vol. 66, no. 4, p. 579, 1996, doi: 10.2307/1170654.

A Appendix A: Comparison of Cyber Resilience Frameworks

This Appendix presents the comparison in eight categories of the identified cyber resilience frameworks.

A comparison of the 18 frameworks found during the conceptualization is shown in Table A.1. The correlative numbers from 1 to 18 shown in Table 3.1 are used to identify the articles in the first column. These 18 frameworks were compared using the following eight properties: audience, profiling, lifecycle, focus, external aspects, implementation order, maturity evolution and type of maturity evolution. The following are definitions of the six mentioned properties:

1. Audience (A): This property refers to the intended final user of the documents. Ideally, for SMEs, the specific audience should be companies or directly SMEs.
2. Profiling (P): This property refers to whether the identified framework requires a customization or selection of a set of policies within it before its implementation or if it is defined to be used as it is. If the document requires customization it is assigned a "yes" in Table A.1, if not, it is assigned a "no". Ideally for SMEs, the framework should not require profiling since this characteristic would require the awareness and knowledge from SMEs to select the appropriate policies and these are not common characteristics that SMEs have
3. Lifecycle (L): This property refers to whether the framework considers the cyber resilience lifecycle (see Figure 1) in its policies or if it does not. This category puts special interest in whether the document considers policies for when there is an incident because it would indicate notions of a "safe-to-fail" approach instead of the traditional "fail-safe" approach [6]. In this sense, the document is assigned a "yes" in Table A.1 if it considers policies or actions for when there is an incident or a "no" when there is none. Ideally for SMEs a framework should consider the complete cyber resilience lifecycle to give them awareness of the importance of preparing and becoming safe-to-fail instead of trying to be fail-safe.
4. Focus (F): This property refers to whether the framework is generalist by considering cyber resilience as a whole or if it specializes in a specific dimension or aspect of cyber resilience. Ideally for SMEs a framework should be generalist since this would give them a complete perspective and let them build cyber resilience in general and not overinvest in specific domains of cyber resilience before investing in other important ones.
5. External aspects (EA): This property refers to whether the framework considers external factors (such as supply chain resilience, collaboration

with third parties, etc.) that could affect cyber resilience or if it focuses only on the internal factors. Similar to some of the previous properties, the ideal for SMEs in external aspects is to contain them since this would let SMEs become more aware of the importance of considering these external aspects when operationalizing cyber resilience.

6. Implementation order (IO): This property refers to whether the framework suggests an order for implementing its defined policies. In this sense, the document is assigned a "yes" in Table A.1 if it suggests an implementation order for the policies or a "no" if it does not. For SMEs the ideal framework would have guidelines on an order in which to implement the suggested policies since this would require less awareness and maturity than having to make the decision by themselves.
7. Policy Maturity Evolution (PME): This property refers to whether the document associates the recommended policy to any kind of maturity model or at least suggests how these policies evolve over time. If the document contained a maturity model or ideas on how the policies progressed the column was marked with a "yes", else it was marked with a "no". Since policies can be understood differently at different maturity states, it is important to give SMEs ideas on how to start their implementation and how to improve it until it is fully operationalized. Therefore, the ideal in this property is to have a "yes".
8. Type of Maturity Evolution (TME): This property was filled with the type of maturity evolution the document included. In this sense, there were three possibilities as suggested by Caralli et al. [98]: capability maturity model, progression model or hybrid. Since as explained before, capability maturity models are usually intended to improve processes that are already implemented and ingrained in the company's culture [98], the ideal for this property is a progression model. A hybrid model would be acceptable as well since it would also allow the companies to understand the most basic form of the policy and how it progresses over time.

Table A.1 shows there are no documents that match all of these ideal properties for a cyber resilience framework for SMEs. In other words, there is no document targeted for SMEs that does not require a selection of policies, that considers the whole cyber resilience lifecycle, has a general cyber resilience approach, considers external aspects of cyber resilience and gives them guidelines for an implementation order and how these policies naturally evolve.

Table A.1 Comparison of cyber resilience frameworks

Ref	A	P	L	F	EA	IO	PME	TME
[101]	Companies	No	No	Information Security and risk management	No	Yes	No	N/A
[95]	Companies	Yes	Yes	Risk management and vulnerability management	No	No	No	N/A
[102]	Companies	Yes	No	Governance of IT and risk management	Yes	Yes	Yes	Capability
[103]	Banks	Yes	Yes	General	Yes	No	No	N/A
[39]	Companies	Yes	Yes	General	No	No	No	N/A
[43]	Federal agencies and Companies	No	Yes	General	Yes	No	No	N/A
[87]	Companies	Yes	Yes	Information Security and risk management	Yes	No	No	N/A
[48]	Federal agencies and Companies	Yes	Yes	General	No	No	No	N/A
[47]	Companies	No	Yes	General	Yes	No	Yes	Capability
[88]	Companies	No	No	General	Yes	No	Yes	Capability
[44]	Companies	No	Yes	General	Yes	No	No	N/A
[104]	Companies	Yes	Yes	General	Yes	No	No	N/A
[85]	Companies	No	No	General	No	No	No	N/A
[64]	Companies	No	No	Governance and risk management	Yes	No	No	N/A
[41]	Critical Infrastructures	Yes	Yes	General	Yes	No	No	N/A
[42]	Companies	No	Yes	General	No	Yes	No	N/A
[94]	Companies	No	Yes	General	Yes	No	Yes	Capability
[37]	Companies	No	Yes	General	Yes	No	No	N/A

B

Appendix B: List of experts and contributions

This Appendix presents a list of the experts with their backgrounds and contributions to the results of this thesis.

Throughout the development and qualitative evaluation of this thesis, several experts of different backgrounds have been interviewed and have contributed to the final results. In this appendix, the list of experts (anonymized with codes and their profiles) are shown in Table B.1.

Table B.1 List of experts and contributions

	Profile	Type of company	Phase II: Conceptual Framework and Implementation Order	Phase III: Progression Model	Phase IV: Simulation Models	Phase V: Evaluation
E1	CISO	University	X	X	X	
E2	Researcher	University	X		X	
E3	CEO	Software development	X		X	
E4	Researcher	University	X	X	X	
E5	Researcher	University	X		X	
E6	Researcher	University	X			
E7	CEO	Logistics and software development		X	X	
E8	CISO	University	X	X	X	
E9	Researcher	University		X	X	
E10	Researcher	University		X	X	
E11	CISO	Energetic distributor		X	X	
E12	Cybersecurity Provider	National Cybersecurity Institute		X	X	
E13	Director of cybersecurity center	Industrial Cybersecurity Center	X	X	X	
E14	Cybersecurity Provider	Cybersecurity consulting		X	X	
E15	Cybersecurity Provider	Cybersecurity consulting and training		X	X	
E16	Cybersecurity Provider	Cybersecurity hardware and software solutions and consulting		X	X	
E17	Technical director	Industrial Cybersecurity Center	X			

E18	Technical member	Industrial Cybersecurity Center	X	
E19	Technical member	Industrial Cybersecurity Center	X	
E20	Technical director	Industrial Cybersecurity Center		X
E21	Cybersecurity Provider	Cybersecurity consulting		X
E22	Cybersecurity Provider	Cybersecurity consulting		X
E23	CISO	Logistics company		X
E24	CEO	Paint manufacturer		X
E25	CEO	Mold Manufacturer		X
E26	CEO	Clinical Pharmacy Organization		X
E27	CISO	Machine tool manufacturer		X
E28	CISO	Machine tool manufacturer		X

C

Appendix C: Decision Tree for Consensus Determination of the Progression Model

This Appendix presents the decision tree used to determine whether there was consensus amongst the experts on the starting maturity level of each domain.

In chapter 4, section 4.4, a progression model is defined based on the interviews made to 11 experts. In order to determine a starting maturity level and a progression type for each policy in the CR-CF, the data obtained from the experts was analyzed. To objectively determine whether a particular set of answers from the experts converged into a consensus the same criteria had to be used for each case. Therefore, a decision tree was constructed.

In this sense, to determine whether there was consensus on the starting maturity for each policy, the mean, the mode, the sub-mode and the confidence intervals for the mean were calculated. The mode was the starting maturity with the greatest number of experts. In case it existed, the sub-mode was a maturity level with the frequency of the mode minus one (e.g., if the mode was level 1 with five experts and level 2 had four experts, level 2 would be the sub-mode). On the other hand, the confidence interval for the mean was calculated for 95% confidence. Although the distribution of the data is unknown, the confidence intervals were calculated assuming normality of the data a common assumption known to have satisfactory results even in non-normal distributions [165]–[167]. The mean and the confidence interval's limits where rounded in order to have integer values and, therefore, no partial maturity levels. Once these calculations were made, a decision on whether there was consensus was taken using the decision tree in Figure C.1.

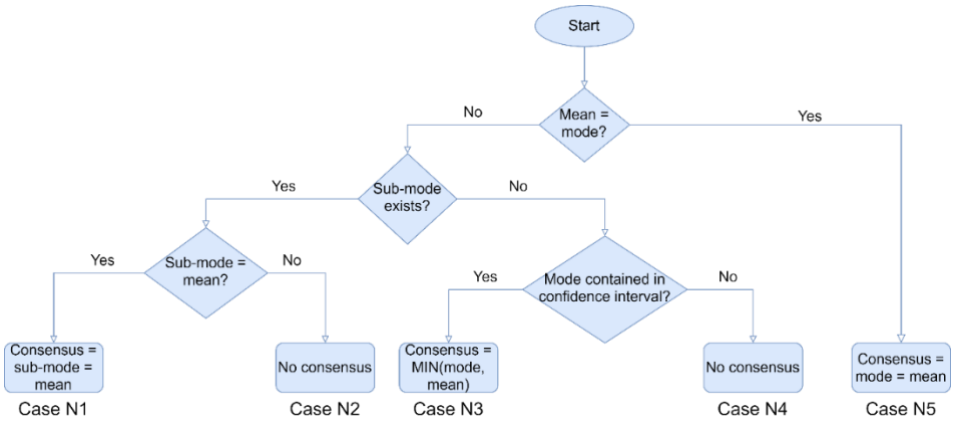

Figure C.1 Quantitative analysis decision tree

As shown in Figure C.1, there are five possible cases for each policy, for clarity, these cases will be numbered in the following description by using N1–N5.

- N1: This case was reached when the rounded mean was different to the mode; the sub-mode existed and was equal to the mean. In this case, the consensus was considered to be the sub-mode because a large group of experts considered this as the starting maturity level for the policy and, the experts who did not, were closer to this starting maturity than to the mode starting maturity.
- N2: This case was reached when the rounded mean was different to the mode; the sub-mode existed but was not equal to the mean. In this case, there was no consensus because neither the mode, nor the sub-mode were around the starting maturity level where the mean expert considered the policy should start.
- N3: This case was reached when the mode and the rounded mean were not equal, there was no sub-mode, and the confidence intervals (CI) contained the mode. In this case, the consensus was the minimum between the mode and the mean. This criterion was applied because the mode and the mean were theoretically not so far apart since it was in the CIs of the mean. The reason for choosing the minimum of the two is that it is more beneficial for cyber resilience building to diversify the investment in policies and to start the implementation as early as possible as suggested by previous studies [136].
- N4: This case was reached when the mode and the rounded mean were different, there was no sub-mode, but the confidence intervals (CI) did not contain the mode. In this case, no consensus was reached because it meant that many experts considered one starting maturity, but that starting maturity was considerably far from most of the other experts' opinion on the policy's starting maturity.
- N5: Finally, this case was reached when the rounded mean was equal to the mode. In this case, the consensus was easily reached because it meant that most experts thought that one starting maturity was predominant and that the experts who diverged from this opinion were not diverging too much from it.

In order to decide whether there was consensus on the progression types the mode and the mode's percentage of agreement were calculated. The mode's percentage of agreement was the percentage of experts who considered the mode

progression type as the main progression type. This means that the mode's frequency was divided by the number of total experts, not the number of total progression types assigned to the policy because experts could describe progressions that were a combination of different progression types. If the percentage of agreement was over 50%, the progression type was considered to be the consensus. If the percentage of agreement was lower, there was no consensus for the policy's progression type. In order to construct an example progression model in the cases with no consensus the mode progression type was used, however, these progressions could be different in different companies and should serve only as examples of possible progressions.

D
Appendix D: Progression Model Data Tables and Consensuses

This Appendix presents the data tables and conclusions from each of the starting maturity states and progression types for each cyber resilience policy. The progression model was then built using these consensuses.

In this Appendix, the complete data obtained from the experts to construct the progression model is presented. This data is used to construct the example progressions in Chapter 4, section 4.4.

The data used to determine consensus for a starting maturity state and the main progression types for each policy is summarized in two tables per domain. The first table of each domain shows the number of experts who voted for each starting maturity state and the information needed to calculate the consensus based on the decision tree shown in Appendix B. After this table, each domain has another table showing the same information but for each progression type. The progression type uses the codes shown in Table D.1. The progression model was constructed based on the consensuses found in the data shown in this section. Whenever there was no clear consensus the mode starting maturity and/or progression type were used to construct the progression model.

Table D.1 Progression types and codes

Progression type	Code
Investment Increase	II
Continuity	C
Specificity	S
Expansion	E
Formalization	F
Independence	I
Optimization	O
Proactivity	P
No progression	N
Technology	T

D.1 Governance

Table D.2 Governance policies' starting maturity

Policy	Policy Code	1	2	3	4	5	Mean	Mode	Sub-Mode	LCI	UCI	Consensus
Develop and communicate a cyber resilience strategy.	G1	4	4	2	1	0	2	1;2	N/A	1	3	2
Comply with cyber resilience-related regulation.	G2	5	2	3	1	0	2	1	N/A	1	3	1
Assign resources (funds, people, tools, etc.) to develop cyber resilience activities.	G3	4	1	5	1	0	2	3	1	1	4	No consensus

Table D.3 Governance policies' progression type

Policy	Policy Code	II	S	E	F	I	O	P	N	Mode	% of Agreement
Develop and communicate a cyber resilience strategy.	G1		1	2	2		2	7		P	64%
Comply with cyber resilience-related regulation.	G2	1		6	1		3	5	1	E	55%
Assign resources (funds, people, tools, etc.) to develop cyber resilience activities.	G3	3		2	2	2	4	2		O	36%

D.2 Risk Management

Table D.4 Risk management policies' starting maturity

Policy	Policy Code	1	2	3	4	5	Mean	Mode	Sub-Mode	LCI	UCI	Consensus
Systematically identify and document the company's cyber risks.	RM1	4	6	1	0	0	2	2	N/A	0	3	2
Classify/prioritize the company's cyber risks.	RM2	0	7	3	1	0	2	2	N/A	1	4	2
Determine a risk tolerance threshold.	RM3	0	5	3	3	0	3	2	N/A	2	4	2
Mitigate the risks that exceed the risk tolerance threshold.	RM4	1	5	4	1	0	2	2	3	1	3	2

Table D.5 Risk management policies' progression type

Policy	Policy Code	II	C	S	E	F	I	O	P	N	Mode	% of Agreement
Systematically identify and document the company's cyber risks.	RM1		2		3	9	1	1	3		F	82%
Classify/prioritize the company's cyber risks.	RM2		2	1	1	7	1	2	2	2	F	64%
Determine a risk tolerance threshold.	RM3					4	1	3	3	3	F	36%
Mitigate the risks that exceed the risk tolerance threshold.	RM4	2		1	5	4	1	3	4		E	45%

D.3 Asset Management

Table D.6 Asset management policies' starting maturity

Policy	Policy Code	1	2	3	4	5	Mean	Mode	Sub-Mode	LCI	UCI	Consensus
Make an inventory that lists and classifies the company's assets and identifies the critical assets.	AM1	6	5	0	0	0	1	1	2	0	3	1
Create and document a baseline configuration for the company's assets.	AM2	1	4	5	1	0	3	3	1	1	4	3
Create a policy to manage the changes in the assets' configurations.	AM3	1	4	2	3	1	3	2	4	2	4	No consensus
Create a policy to periodically maintain the company's assets.	AM4	4	5	1	0	1	2	2	1	1	3	2
Identify and document the internal and external dependencies of the company's assets.	AM5	1	5	3	2	1	3	2	N/A	2	4	2

Table D.7 Asset management policies' progression type

Policy	Policy Code	C	S	E	F	I	O	P	N	T	Mode	% of Agreement
Make an inventory that lists and classifies the company's assets and identifies the critical assets.	AM1		6	4	4			2		3	S	55%
Create and document a baseline configuration for the company's assets.	AM2		1	2	4	1	1	3		4	F;T	36%
Create a policy to manage the changes in the assets' configurations.	AM3		1	3	4	1	1	3		4	F;T	36%
Create a policy to periodically maintain the company's assets.	AM4	2		1	4	1	2	6	1	1	P	55%
Identify and document the internal and external dependencies of the company's assets.	AM5	1		4	5	1	1	5		3	F;P	45%

D.4 Threat and Vulnerability Management

Table D.8 Threat and vulnerability management policies' starting maturity

Policy	Policy Code	1	2	3	4	5	Mean	Mode	Sub-Mode	LCI	UCI	Consensus
Identify and document the company's threats and vulnerabilities.	TVM1	3	4	4	0	0	2	2;3	1	1	3	2
Mitigate the company's threats and vulnerabilities.	TVM2	2	1	6	2	0	3	3	N/A	1	4	3

Table D.9 Threat and vulnerability management policies' progression type

Policy	Policy Code	II	C	S	E	F	I	O	P	N	T	Mode	% of Agreement
Identify and document the company's threats and vulnerabilities.	TVM1	1	2		5	7	1		6	1		F	64%
Mitigate the company's threats and vulnerabilities.	TVM2	2	2	1	3	3	1	4	3		1	O	36%

D.5 Incident Analysis

Table D.10 Incident analysis policies' starting maturity.

Policy	Code	1	2	3	4	5	Mean	Mode	Sub-Mode	LCI	UCI	Consensus
Assess and document the damages suffered after an incident.	IA1	1	6	3	0	1	2	2	N/A	1	4	2
Analyze the suffered incidents to find as much information as possible: causes, methods, objectives, point of entry, etc.	IA2	2	2	5	2	0	3	3	N/A	2	4	3
Evaluate the company's response and response selection to the incident.	IA3	0	1	2	2	6	4	5	N/A	3	6	5
Identify lessons learned from the previous incidents and implement measures to improve future responses, response selections, and risk management.	IA4	0	1	6	2	2	3	3	N/A	1	3	3

Table D.11 Incident analysis policies' progression type

Policy	Code	II	C	S	E	F	I	O	P	N	Mode	% of Agreement
Assess and document the damages suffered after an incident.	IA1	1		3	1	6			3	1	F	55%
Analyze the suffered incidents to find as much information as possible: causes, methods, objectives, point of entry, etc.	IA2		1	5	3	4	1		4		S	45%
Evaluate the company's response and response selection to the incident.	IA3	1		1		3		1		6	N	55%
Identify lessons learned from the previous incidents and implement measures to improve future responses, response selections, and risk management.	IA4				1	5			3	3	F	45%

D.6 Awareness and Training

Table D.12 Awareness and training policies' starting maturity.

Policy	Policy Code	1	2	3	4	5	Mean	Mode	Sub-Mode	LCI	UCI	Consensus
Define and document training and awareness plans.	AT1	3	1	6	1	0	2	3	N/A	1	4	3
Evaluate the gaps in the personnel skills needed to perform their cyber resilience roles and include these gaps in the training plans.	AT2	0	2	2	7	0	3	4	N/A	2	5	4
Train the personnel with technical skills.	AT3	2	3	4	2	0	3	3	2	2	3	3
Raise the personnel's awareness through their training programs.	AT4	3	4	3	1	0	2	2	1;3	1	3	2

Table D.13 Awareness and training policies' progression type.

Policy	Policy Code	II	C	S	E	F	I	O	P	N	Mode	% of Agreement
Define and document training and awareness plans.	AT1			6	2	2		1	2		S	55%
Evaluate the gaps in the personnel skills needed to perform their cyber resilience roles and include these gaps in the training plans.	AT2		4	2		1	1		2	3	C	36%
Train the personnel with technical skills.	AT3	1	1	6	1	2		1	3		S	55%
Raise the personnel's awareness through their training programs.	AT4		3	3		6	1	1	2		F	55%

D.7 Information Security

Table D.14 Information security policies' starting maturity.

Policy	Policy Code	1	2	3	4	5	Mean	Mode	Sub-Mode	LCI	UCI	Consensus
Implement measures to protect confidentiality (e.g., access control measures, network segmentation, cryptographic techniques for data and communications, etc.)	IS1	6	2	3	0	0	2	1	N/A	0	3	1
Implement integrity checking mechanisms for data, software, hardware and firmware.	IS2	4	4	3	0	0	2	1;2	3	1	3	2
Ensure availability through backups, redundancy, and maintaining adequate capacity.	IS3	5	3	3	0	0	2	1	N/A	1	3	1

Table D.15 Information security policies' progression type.

Policy	Policy Code	II	S	E	F	O	P	T	Mode	% of Agreement
Implement measures to protect confidentiality (e.g., access control measures, network segmentation, cryptographic techniques for data and communications, etc.)	IS1		5	3	4		1	8	T	72%
Implement integrity checking mechanisms for data, software, hardware and firmware.	IS2		3	3	4	1	2	7	T	64%
Ensure availability through backups, redundancy, and maintaining adequate capacity.	IS3	1	3	5	4		1	7	T	64%

D.8 Detection Processes and Continuous Monitoring

Table D.16 Detection processes and continuous monitoring policies' starting maturity.

Policy	Policy Code	1	2	3	4	5	Mean	Mode	Sub-mode	LCI	UCI	Consensus
Actively monitor the company's assets (e.g., by implementing controls/sensors, IDS, etc.)	DPM1	1	7	3	0	0	2	2	N/A	0	4	2
Define a detection process that specifies when to escalate anomalies into incidents and notifies the appropriate parties according to the type of detected incident.	DPM2	0	2	6	3	0	3	3	N/A	2	5	3

Table D.17 Detection processes and continuous monitoring policies' progression types

Policy	Policy Code	C	S	E	F	O	P	T	Mode	% of Agreement
Actively monitor the company's assets (e.g., by implementing controls/sensors, IDS, etc.)	DPM1	1	2	5	1	3	2	5	E;F	45%
Define a detection process that specifies when to escalate anomalies into incidents and notifies the appropriate parties according to the type of detected incident.	DPM2			2	5	1	3	3	F	45%

D.9 Business Continuity Management

Table D.18 Business continuity management policies' starting maturity.

Policy	Policy Code	1	2	3	4	5	Mean	Mode	Sub-Mode	LCI	UCI	Consensus
Define and document plans to maintain the operations despite different scenarios of adverse situations.	BCM1	0	3	6	2	0	3	3	N/A	1	4	3
Define and document plans to respond to and recover from incidents that include recovery time objectives and recovery point objectives.	BCM2	1	1	8	1	0	3	3	N/A	1	5	3
Periodically test the business continuity plans to evaluate their adequacy and adjust them to achieve the best possible operations under adverse situations.	BCM3	0	0	1	9	1	4	4	N/A	2	6	4

Table D.19 Business continuity management policies' progression type.

Policy	Policy Code	II	C	S	E	F	O	P	N	Mode	% of Agreement
Define and document plans to maintain the operations despite different scenarios of adverse situations.	BCM1				6	6	1	3		E;F	55%
Define and document plans to respond to and recover from incidents that include recovery time objectives and recovery point objectives.	BCM2				6	6	1	2	1	E;F	55%
Periodically test the business continuity plans to evaluate their adequacy and adjust them to achieve the best possible operations under adverse situations.	BCM3	1	3	1	1	1	1	2	3	C;N	27%

D.10 Information Sharing and Communication

Table D.20 Information sharing and communication starting maturity

Policy	Policy Code	1	2	3	4	5	Mean	Mode	Sub-mode	LCI	UCI	Consensus
Define information sharing and cooperation agreements with external private and public entities to improve the company's cyber resilience capabilities.	SHC1	0	0	5	3	3	4	3	N/A	3	5	3
Define and document a communication plan for emergencies that takes into account the management of public relations, the reparation of the company's reputation after an event, and the communication of the suffered incident to the authorities and other important third parties.	SHC2	1	1	6	3	0	3	3	N/A	2	4	3
Establish collaborative relationships with the company's external stakeholders (e.g., suppliers) to implement policies that help each other's cyber resilience goals.	SHC3	1	1	6	3	0	3	3	N/A	2	4	3

Table D.21 Information sharing and communication progression type.

Policy	Policy Code	S	E	F	I	P	N	T	Mode	% of Agreement
Define information sharing and cooperation agreements with external private and public entities to improve the company's cyber resilience capabilities.	SHC1		1	4		4	3		F;P	36%
Define and document a communication plan for emergencies that takes into account the management of public relations, the reparation of the company's reputation after an event, and the communication of the suffered incident to the authorities and other important third parties.	SHC2	5	2	4		2		1	S	45%
Establish collaborative relationships with the company's external stakeholders (e.g., suppliers) to implement policies that help each other's cyber resilience goals.	SHC3		3	6	1	3	1		F	55%

E

Appendix E: Complete Case Study Process

This Appendix presents the complete information collected from one of the case studies to serve as an example and showcase the decisions companies made using the CR-OF as their means of operationalizing cyber resilience.

In order to showcase the usage of the CR-OF in the decision-making process for cyber resilience operationalization in a more detailed manner, this appendix shows the complete case study process with the paint manufacturing company from Spain. This complete process will serve as an example of the process followed in the six case studies that are described in a summarized manner in chapter 5, section 5.1.

The first step of the case study was to contact their CEO, who kindly agreed to participate in the research. This person was contacted because he is in charge of the cybersecurity decisions in the company which is the common criteria used in every case study. By contacting a decision-maker in cyber resilience operationalization the usage of the proposed tools can be agreed upon and deployed in the company. At the same time, the decision-maker can have a better perspective of the usefulness and completeness of the tools.

During the first meeting, general questions about the company were asked to make sure the information found publicly about the company was correct. In this meeting the process of the CR-OF was explained to the decision-maker as well as the results that aid companies follow that process. The idea of this first meeting was to agree on the next steps the company should take and thus start following the CR-OF to test if it aided them in their decision-making.

The first tool every company had to use was the CR-SAT since it is the tool that lets companies know their current situation in order to start improving it. In the case of this case study, the company used the CR-SAT and got the maturity states shown in Table E.1.

Table E.1 Maturity level per policy for the Spanish paint manufacturer

Code	**Policy**	Maturity Level
G1	Develop a cyber resilience strategy.	5
G2	Comply with cyber resilience-related regulation.	3
G3	Assign resources (funds, people, tools, etc.) to develop cyber resilience activities.	5
RM1	Systematically identify and document the company's cyber risks.	3
RM2	Classify/prioritize the company's cyber risks.	3
RM3	Determine a risk tolerance threshold.	3
RM4	Mitigate the risks that exceed the risk tolerance threshold.	4
AM1	Make an inventory that lists and classifies the company's assets and identifies the critical assets.	3

AM2	Create and document a baseline configuration for the company's assets.	3
AM3	Create a policy to manage the changes in the assets' configurations.	3
AM4	Create a policy to periodically maintain the company's assets.	4
AM5	Identify and document the internal and external dependencies of the company's assets.	3
TVM1	Identify and document the company's threats and vulnerabilities.	3
TVM2	Mitigate the company's threats and vulnerabilities.	4
IA1	Assess and document the damages suffered after an incident.	3
IA2	Analyze the suffered incidents to find as much information as possible: causes, methods, objectives, point of entry, etc.	5
IA3	Evaluate the company's response and response selection to the incident.	5
IA4	Identify lessons learned from the previous incidents and implement measures to improve future responses, response selections, and risk management.	5
AT1	Define and document training and awareness plans.	3
AT2	Evaluate the gaps in the personnel skills needed to perform their cyber resilience roles and include these gaps in the training plans.	0
AT3	Train the personnel with technical skills.	4
AT4	Raise the personnel's awareness through their training programs.	4
IS1	Implement measures to protect confidentiality (e.g. access control measures, network segmentation, cryptographic techniques for data and communications, etc.)	3
IS2	Implement integrity checking mechanisms for data, software, hardware and firmware.	2
IS3	Ensure availability through backups, redundancy, and maintaining adequate capacity.	4
DPM1	Actively monitor the company's assets (e.g. by implementing controls/sensors, IDS, etc.)	4
DPM2	Define a detection process that specifies when to escalate anomalies into incidents and notifies the appropriate parties according to the type of detected incident.	3
BCM1	Define and document plans to maintain the operations despite different scenarios of adverse situations.	3
BCM2	Define and document plans to respond to and recover from incidents that include recovery time objectives and recovery point objectives.	3
BCM3	Periodically test the business continuity plans to evaluate their adequacy and adjust them to achieve the best possible operations under adverse situations.	0
SHC1	Define information sharing and cooperation agreements with external private and public entities to improve the company's cyber resilience capabilities.	3
SHC2	Define and document a communication plan for emergencies that takes into account the management of public relations, the reparation of the company's reputation after an event, and the communication of the suffered incident to the authorities and other important third parties.	3
SHC3	Establish collaborative relationships with the company's external stakeholders (e.g. suppliers) to implement policies that help each other's cyber resilience goals.	3

During the process of self-assessing, a second meeting was held in which the company had already self-assessed but were asked to fill in the evidences they considered when selecting each policy's maturity level. The evidences can serve as examples of how each company interprets the scales in the progression model that are in the CR-SAT and serve as proof that the selected maturity levels are

selected based on those scales. Thus, this meeting was important for the case study to ascertain that the company was able to understand the scales and identify in one of the maturity states. The evidences per policy given by the company are shown in Table E.2.

Table E.2 Evidences per cyber resilience policy in the Spanish paint manufacturer

Code	Evidences
G1	A minimum of one meeting is held annually to discuss and improve the company's cybersecurity strategy. In these meetings the lessons learned from the previous year and points of improvement to continue are discussed.
G2	There are not many laws related to cyber resilience in Spain. The most applicable is the GDPR and we do not manage too much information. We do our best to keep supplier and customer data protected according to that law, but we do not do internal audits.
G3	Since we have had two incidents, we have managed security budgets flexibly. Allocating resources to what is needed to be more secure.
RM1	The cybersecurity provider is in charge of identifying risks to the company's assets. There is no systematic procedure in the company to do this, but we have a list of risks based on reports from the cybersecurity vendor.
RM2	We rank the risks from the list delivered by the cybersecurity provider, but we do not go as far as quantifying the risks. Rather according to what they tell us to prioritize as having the greatest impact.
RM3	By not having the risks quantified we rely on that potential impact of incidents to determine the level of tolerance we may have to accept or decide to act on a risk.
RM4	We try to mitigate and take action whenever we have identified a risk that could harm us. Through the help of the cybersecurity provider, we managed to mitigate almost all of the high priority risks we managed to identify.
AM1	Invoices for the acquisition of assets that are in the company are retained. Through these invoices a detailed inventory of all the company's assets is kept and their location is known since they are all in the same physical space.
AM2	There is no document with the base configurations of the company's assets, but the supplier configures the assets according to the team's needs in a standard way.
AM3	When a change in a configuration or equipment is required, the supplier acts as requested. There is no traceable record, but changes to configurations are known.
AM4	All systems are updated as soon as possible and preventive maintenance schedules are scheduled from time to time.
AM5	There are not many systems in the company, so the internal dependencies between them are easily known. The external ones have not been studied.
TVM1	The cybersecurity provider periodically sends out a bulletin informing the company of new vulnerabilities discovered in the systems. For this they have a list of vulnerabilities in their assets.
TVM2	The risk is not yet quantified and vulnerabilities are considered as risks but are not quantified. Vulnerabilities that may represent a high impact are mitigated in the same way that risks that meet this condition are mitigated.
IA1	After the 2 incident experiences of the last year the company knows the losses it had due to the incidents that occur.
IA2	After the last incident a forensic service was contracted and taken to the Ertzaintza. The forensic analysis done by the contracted company searched for all possible information so it is quite complete.
IA3	In order to improve more and more, the company analyzes whether its response was adequate and thinks about how to improve its response to incidents on future occasions.
IA4	It documents what happened and takes into account the lessons learned from incidents and forensic analysis to improve in the future.
AT1	There is a generalized plan that focuses primarily on making staff aware of what not to do to try to prevent such actions from causing an incident.

AT2	There is no customization of training plans, so there has been no assessment of any training gaps that may exist in the staff.
AT3	General technical training is given to systems personnel. However, they are still general plans for that profile. The training of the rest of the employees is mainly awareness training.
AT4	From time to time the systems staff reminds all employees of those issues that have to be taken into account to keep the systems secure. Mainly these communications are through e-mails.
IS1	There is oversight of the company's access control and permissions management. Everything is set up so that only authorized persons have access to important documents, especially customer information.
IS2	No special integrity measures are used in the company.
IS3	There is a system of multiple backups including one on a physical hard drive that the CEO takes home every day. In addition, the company's main systems have redundant systems in case something happens to be able to use the copy to continue with its activity.
DPM1	There are automatic monitoring systems that generate automatic alerts in case any indicator has an undesired behavior.
DPM2	When something happens, it is kept in mind to call the supplier or the systems manager and to inform the Ertzaintza when it is an attack. However, no specific plans have been developed for each type of incident.
BCM1	There are no documented plans, but it is known how to act in the event of an incident in the company to try to maintain operations.
BCM2	There are no documented plans but there are ideas on how to recover after an incident.
BCM3	Continuity plans are not tested. Even the backup that Gerardo physically carries is in doubt as to whether or not it works.
SHC1	The only relationships with external entities are personal relationships between employees of both companies. There is nothing formalized.
SHC2	There is a general communication plan included in the general detection plan mentioned above. There are no formal documents but it is known how to act.
SHC3	This has been considered in some of the incidents: communicate to external agents about the incident suffered so that they take it into account and take the necessary measures but it has never been done formally. Communication with them is informal as well as with other external entities.

After filling the questions in the CR-SAT, the tool calculated the average of maturity level per domain in this company using an arithmetic mean. The radar graph showing these averages that the CR-SAT showed as an output is shown in Figure E.1.

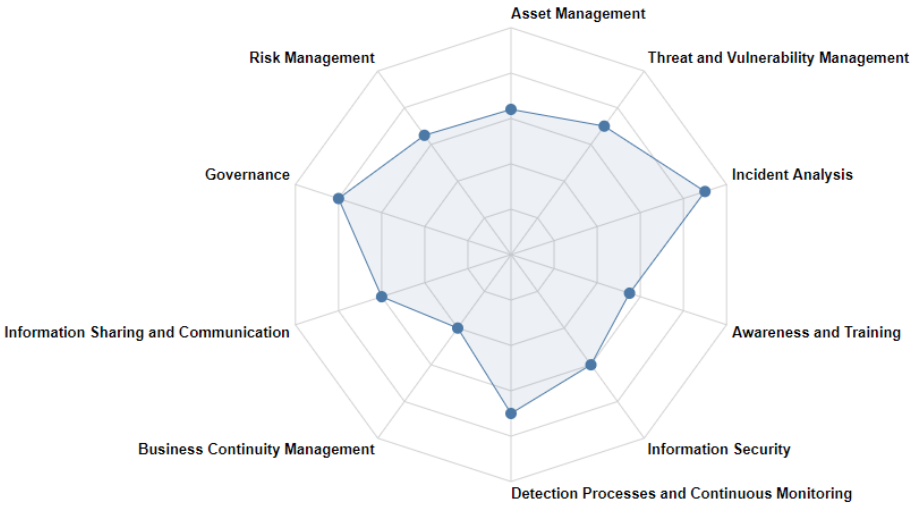

Figure E.1 Radar graph with average maturity level per domain

At the same time, the CR-SAT gave the company a full report of the maturity levels shown in Table E.1 in several radar and bar charts (one chart per domain) as shown in Figure E.2. Using the information shown in the charts the company could visually see their weaknesses and strengths. This information was their first approach to decide in which domain and specific policies they wished to improve upon.

In this case, the company studied their radar charts and determined they had weaknesses in the business continuity management and awareness and training domains. In these domains the company noticed they had policies with a maturity level of zero and almost immediately decided they wanted to improve. However, overall the radar charts look balanced and with similar maturity levels on every domain. Although the company does have weaknesses in those domains, they could improve in whichever domain and policy they wished since they have not fallen behind by much in any domain.

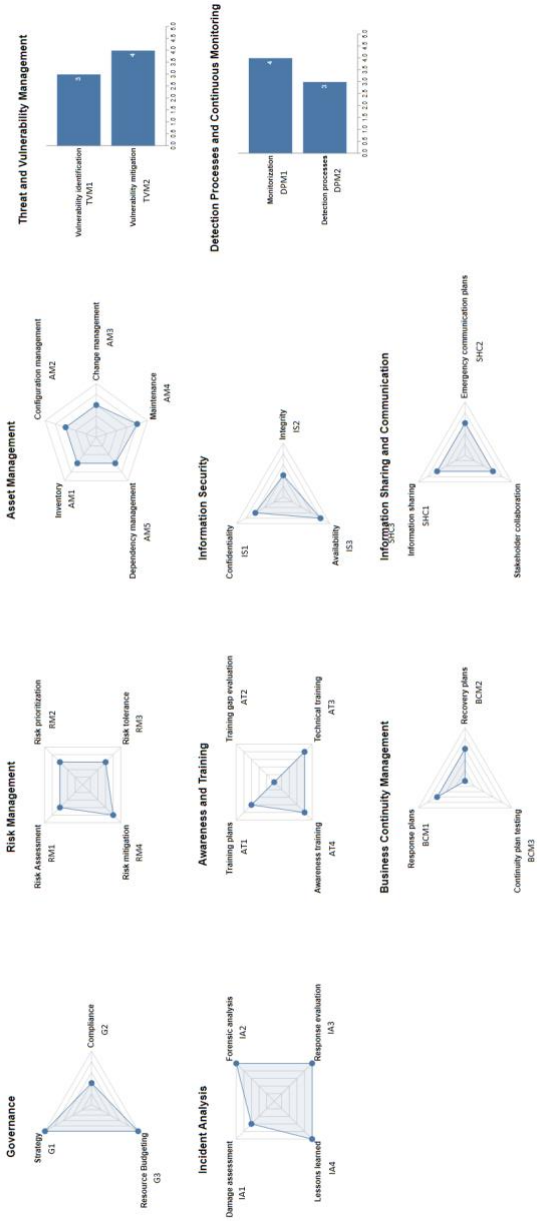

Figure E.2 Detailed report from the CR-SAT

Using these results and a feature in the CR-SAT that showed all of the policies in which they had less than a maturity level of 5 with their current maturity and the description of the next maturity level in the progression model, the company had to decide which policies they wished to improve in a third meeting. Table E.3 shows the policies the company decided to improve.

Table E.3 Cyber resilience policies the Spanish paint manufacturer decided to improve

Code	Next Steps description
RM2	Risks are calculated based on their impact and probability. The numerical risk values are considered when prioritizing risks.
RM3	The risk tolerance threshold is documented as a value of risk (impact x probability).
AM5	The dependencies are systematically identified for all of the company's assets and documented in the dependency list.
TVM1	There is a systematic procedure (i.e. pen testing) used to identify all the threats and vulnerabilities associated to the company's assets.
TVM2	All threats and vulnerabilities are mitigated (including newly discovered ones) when they exceed the latest update of the risk tolerance threshold.
AT1	There are plans defined according to different profiles of the employees.
AT4	The company systematically and periodically does awareness training courses or communications for the employees such as spam exercises, training sessions, etc.
IS1	The company has implemented the most advanced confidentiality measures possible (e.g. encryption of data and communications).
DPM2	There is a documented plan with clear instructions on what to do when there is an incident in the company.
BCM3	Business continuity plans are tested in order to determine their effectivity in the situations they are meant to be used.
SHC1	There are documented, formal and well-defined relationships between the company and some external entities to share information about cyber resilience.
SHC3	There are documented, formal and well-defined relationships between the company and some external stakeholders to cooperate and follow certain guidelines about cyber resilience.

Although the company had a determination to work in business continuity and awareness and training, they also wanted to improve several other policies. They also followed the process as agreed and tried to prioritize the policies they wished to improve by using the implementation order. Figure E.3 highlights in colors the policies the company wanted to improve in the implementation order.

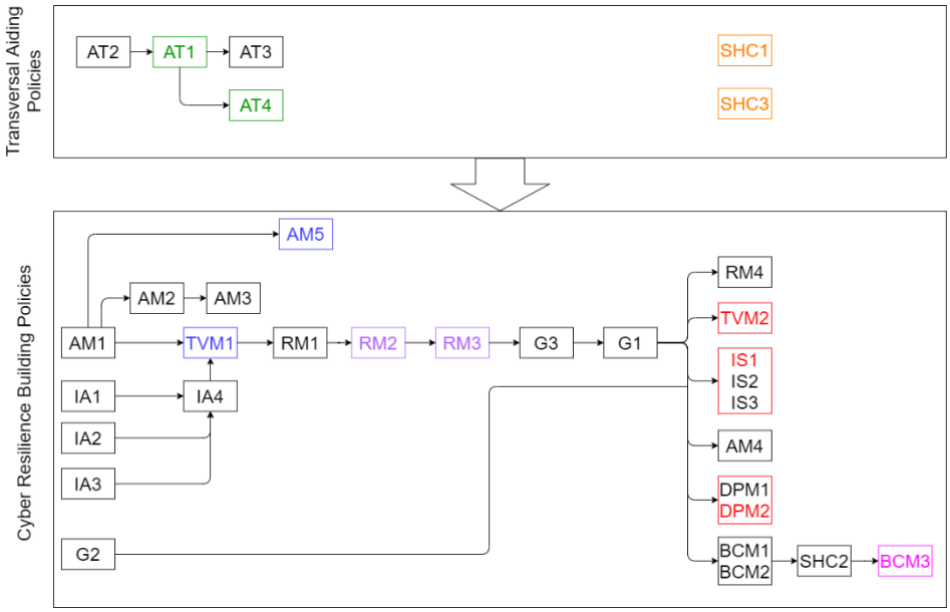

Figure E.3 Prioritization of the policies the company wanted to improve

Using the implementation order, the company ended up leaning towards the improvement of their identification of threats to improve their risk management. Moreover, they decided to start quantifying their risk management and identifying their dependencies to also know more about the possible impact of their risks.

In addition, the company decided to improve their mitigation of the threats and vulnerabilities they will discover when they improve their identification of threats. They also wanted to improve their confidentiality measures by encrypting the backup drive that goes outside of the company every day.

In the transversal aiding policies the company wanted to formalize their training plans, especially the awareness plans for the personnel. They also wished to start formalizing collaboration relationships with their clients, suppliers and other companies in the region.

Finally, the company wanted to improve in their business continuity and they decided to improve this in two different ways. The first one was to start testing their response and recovery plans. This way, they wanted to make sure

they could at least recover the information from the backups and backup drive. The second way they wished to improve their business continuity is by having well defined detection processes so that the time between the discovery of an incident and the beginning of the response plan is minimized. In this sense, the company decided to start improving their detection processes by formalizing and documenting the process in the different scenarios it could occur.

At this point in the research, all the case studies were finished after the decision-making process. Longitudinal studies with sample information months or years after the beginning of the implementation of the CR-OF could be made to see the effect of using the CR-OF over extended periods and see if companies are able to keep using it over these periods. However, these studies are not made within the span of this thesis.

After the using the CR-OF and the case study was finished a last meeting with the CEO of the company was held to receive the company's feedback. They saw great usefulness in the tool and pointed out the importance of the tool highlighting continuity after an incident has happened. They considered this important because of the incidents they have suffered and the hard lessons they learned from suffering those incidents. The CEO pointed out that the usage of the tool was very interesting to them and that they would probably use it with the help of their cybersecurity provider, since in some cases they would not have the capability to improve on certain domains or policies by themselves. Thus, they considered that the tool was useful, but that it is not a substitute and should be complementary to a cybersecurity provider.

Regarding the completeness of the tool, the company was pleased and thought that everything they could have asked for was there. They considered that the tool included aspects of cyber resilience and cybersecurity they had not considered themselves in the company (such as testing their continuity plans) and, thus, to their perspective, it is a very complete tool.

Publications

In this chapter the publications achieved as a result of this research are included. First, papers directly related to the results of this PhD thesis are presented. Secondly, other papers of the author of this PhD thesis are listed. The publications are classified by the different types of publications namely journal publications and conference publications.

P1. PUBLICATIONS RELATED TO THE THESIS

P1.1 SCIENTIFIC JOURNAL PUBLICATIONS

Authors: Carías, J. F.; Borges, M. R. S.; Labaka, L.; Arrizabalaga, S. & Hernantes, J.

Title: Systematic Approach to Cyber Resilience Operationalization in SMEs

Journal: IEEE Access

Year: 2020 **Volume**: 8 **Pages**: 174200- 174221

Indexed in: JCR (Q2)

Authors: Carías, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J.

Title: Cyber Resilience Progression Model

Journal: Applied Sciences

Year: 2020 **Volume**: 10 (21) **Pages**: 7393

Indexed in: JCR (Q2)

Authors: Carías, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J

Title: Defining a Cyber Resilience Investment Strategy in an Industrial Internet of Things Context

Journal: Sensors (Switzerland)

Year: 2019 **Volume**: 9 **Pages**: 80741-80762

Indexed in: JCR (Q1)

Authors: Carías, J. F., Arrizabalaga, S., Labaka, L. & Hernantes, J

Title: Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs

Journal: IEEE Access

Year: 2021 **Volume**: 19(1) **Pages**: 138

Indexed in: JCR (Q2)

P1.2 CONFERENCE PUBLICATIONS

Authors: Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J.

Title: The Order of the Factors DOES Alter the Product: Cyber Resilience Policies' Implementation Order.

Conference: Computational Intelligence in Security for Information Systems Conference, CISIS.

Place and date: Burgos, Spain. 2020. September 16th – 18th

Authors: Carias, J. F., Arrizabalaga, S., & Hernantes, J.

Title: Cyber Resilience Self-Assessment and Strategic Planning Tool.

Conference: The International Emergency Management Society Conference (TIEMS)

Place and date: (Online). 2020. November 30th – December 4th

Authors: Carias, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J.

Title: An approach to the modeling of cyber resilience management

Conference: Global Internet of Things Summit, GIoTS

Place and date: Bilbao, Spain. 2018. June 4th – 7th

Authors: Carias, J.F., Labaka, L., Sarriegi, J.M., Tapia, A. & Hernantes, J.

Title: The Dynamics of Cyber Resilience Management.

Conference: Information Systems for Crisis Response and Management, ISCRAM

Place and date: Valencia, Spain. 2019. May 19th – 22nd

Authors: Carias, J. F., Iturriza, M., Arrizabalaga, S., & Hernantes, J

Title: Cyber Resilience Awareness Training Cyber Ranges.

Conference: Information Technology in Disaster Risk Reduction, ITDRR

Place and date: Sofia, Bulgaria. 2020. December 3rd – 4th

P2. OTHER PUBLICATIONS

P2.2 CONFERENCE PUBLICATIONS

Authors: Figueroa, S., Carias, J. F., Anorga, J., Arrizabalaga, S., & Hernantes, J.

Title: A RFID-based IoT Cybersecurity Lab in Telecommunications Engineering

Conference: Technologies Applied to Electronics Teaching, TAEE

Place and date: Tenerife, Spain. 2018. July 20th - 22nd

Authors: Serrano, N., Blanco, C., Carías, J. F., & Reina, E.

Title: Information from Automated Evaluation in an Engineering School.

Conference: International Conference on Higher Education Advances, HEAd

Place and date: Valencia, Spain. 2018. June 20th-22nd.