IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 21, 2020, accepted September 14, 2020, date of publication September 23, 2020, date of current version October 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3026063

Systematic Approach to Cyber Resilience Operationalization in SMEs

JUAN FRANCISCO CARÍAS[1], MARCOS R. S. BORGES[1], (Member, IEEE), LEIRE LABAKA[1], SAIOA ARRIZABALAGA[1,2], AND JOSUNE HERNANTES[1]

[1]TECNUN, School of Engineering, University of Navarra, 20018 Donostia-San Sebastian, Spain
[2]CEIT, 20018 Donostia-San Sebastian, Spain

Corresponding author: Juan Francisco Carías (jfcarias@tecnun.es)

This work was supported by the Basque Government under Project ELKARTEK 2019 KK-2019/00072.

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 traditional cybersecurity approach of protecting against known threats cannot withstand the rapidly evolving technologies and threats used by cybercriminals. 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, and thus, the study presents a framework with a corresponding implementation order for SMEs that could help them implement cyber resilience practices. The framework is the result of using a variation of Design Science Research in which Grounded Theory was used to induce the most important actions required to implement cyber resilience and an iterative evaluation from experts to validate the actions and put them in a logical order. Therefore, this study proposes that the framework could benefit SME managers to understand cyber resilience, as well as help them start implementing it with concrete actions and an order dictated by the experience of experts. This could potentially ease cyber resilience implementation for SMEs by making them aware of what cyber resilience implies, which dimensions it includes and what actions can be implemented to increase their cyber resilience.

INDEX TERMS Cyber resilience, design science research (DSR), framework, grounded theory, guidelines, SMEs.

I. INTRODUCTION

Cyber threats are one of the main risks companies face today [1], [2], and they affect a large percentage of companies every year, especially Small and Medium-Sized Enterprises (SMEs) [1]–[4]. The economic impact of cyber incidents can cost between hundreds of thousands of euros to the millions per company and per year in the European Union (EU) [5]. Globally this economic impact can vary from the lowest average of 16,400 euros to the highest average of 14.1 million euros [5]. This means that for an SME, a successful cyber-attack 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 [6]. 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 [7], [8]. 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 [7], [9], [10] and are crucial to the economic development of these regions due to their creation of jobs [11]–[13]. However, SMEs often have scarce resources [7], [10], [13]–[16], and limited workforce focused on this issue to protect against cyber threats [14], [17] which reinforces their cybersecurity problem.

On the other hand, the traditional cybersecurity approach of an intended "fail-safe" protection cannot withstand the ever-evolving environment of the cyber risks and technology [8], [18], [19]. Therefore, the traditional cybersecurity point

The associate editor coordinating the review of this manuscript and approving it for publication was Luis Javier Garcia Villalba.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

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 [19]. 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 [20]–[23]. Cyber resilience's main purpose, opposite to traditional views of cybersecurity, is to prepare the company to be a ''safe-to-fail'' system in order to maintain business continuity despite any type of adverse situations, including unexpected and unknown ones [19]–[21], [24].

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 [20], [25], [26] among other dimensions for which SMEs usually do not have assigned resources [14], [17]. 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. [25], [27], [28] that were not usually considered in traditional cybersecurity [29], [30]. 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 [7], [10], [14], [15]. 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 [7], [9], [10] and their shortcomings for the implementation of cyber resilience [7], [10], [14], [15], [17], an SME oriented approach to cyber resilience is needed. Currently, several cybersecurity and cyber resilience frameworks exist in the literature [25], [27], [31]. However, these frameworks are not designed specifically for SMEs since they often include hundreds of specific policies [23], [25], [26], [32] that might not all be applicable for SMEs. Thus, it is relevant to define a cyber resilience framework oriented for SMEs.

Thus, the aim of this study is to present a cyber resilience framework for SMEs and guidelines on how to implement it. This framework will summarize the different dimensions that cyber resilience implies and the policies that SMEs need to implement them. In addition, the guidelines will be presented in the form of an implementation order with the objective to help SMEs address the framework's policies in an order that has a basis on experience. The combination of the framework and guidelines for implementation are from hereafter referred to as ''framework''.

This study's framework could potentially help SMEs understand cyber resilience, be aware of the dimensions and actions it requires operationalize and have clear guidelines on a possible order in which they could implement these actions. Thus, the framework would aid in reducing the challenges in the cyber resilience operationalization for SMEs. Moreover, this is unlike other solutions [23], [25], [32] in which resources would have to be invested into the acquisition of this information on which actions need to be implemented, and in which order does it make sense to implement them in order to operationalize cyber resilience.

Therefore, the contributions of this paper are:

- The definition of a complete yet synthesized cyber resilience framework, with the essential cyber resilience domains and policies needed for its operationalization.
- A high-level implementation order to serve as guidelines for SMEs to better understand the relationship between the framework's domains and therefore as a starting point for their cyber resilience operationalization process.

These contributions, although based on the literature and practitioners' experience, still have the limitation of a theoretical scope and should be tested and iteratively improved in real situations. These contributions are also limited to aid SMEs that are starting their operationalization process and that currently have limited knowledge in cyber resilience. This limitation is because more experienced companies in the field, in theory, would require frameworks that include more details and nuances within the cyber resilience policies such as the ones in the frameworks of the current literature [23], [25], [32].

In the following section, a literature review shows the state of the art of cyber resilience frameworks in the current literature. Section 3 explains the methodology used in this research. Section 4 presents how the methodology was applied to obtain the cyber resilience framework. Section 5 contains the development process and the final consensus on a possible implementation order. Section 6 contains suggestions on how to use the framework. Section 7 elaborates on the results of the qualitative evaluation of the usefulness of the framework. Section 8 has a discussion on the importance and uses of this framework for SMEs. Finally, Section 9, highlights the conclusions drawn from this paper and future lines of research.

II. STATE OF THE ART

With the evolution of technology, information security evolved into the broader concept of cybersecurity [33]. The concept of cybersecurity referred to the protection not only of the Confidentiality, Integrity and Availability (CIA triad) of information resources but also to other assets [33]. For instance, remotely turning off the security measures (cameras, alarms, etc.) in order to enter and burgle money from a small shop would not directly affect the CIA triad, so it is not an information security concern, but it is a cybersecurity one [33]. However, over the past few decades, information security and cybersecurity have been mostly based on protection and detection; it is not until this decade that incident response has become a concern [30], [34]. Moreover, these

FIGURE 1. Cyber Resilience Lifecycle.

concepts rely most of the time on technology and keeping humans and human processes out of the equation [29].

These concerns about including the anticipate, detect, withstand, recover, and evolve [20], [23], [25], [27] lifecycle and the inclusion of humans into cybersecurity have led to an emerging new approach called cyber resilience [20], [22], [24], [27], [28].

Although some authors consider cyber resilience a part of cybersecurity that is concerned with response [22], [35], [36], other authors consider cyber resilience a more holistic concept that includes the whole lifecycle (Figure 1) and that includes strategic and human processes into cybersecurity [20], [23], [27], [28]. This ambiguity of the cyber resilience concept may be due to the continuously changing cybersecurity concept throughout the past few decades [30], [35], [37]. However, there are clear differences between the cybersecurity and cyber resilience concepts. The main differences include [21]:

- The objective of maintaining business continuity rather than protecting Information Technology (IT) systems.
- The intention of being safe-to-fail rather than fail-safe.
- A holistic (network of organizations) approach rather than the atomistic (one organization) approach.

Therefore, this article adopts the idea of cyber resilience as a holistic approach to cybersecurity. In this sense the article adopts the following definition of cyber resilience: ''Ability of a process, business, organization or nation to anticipate, [detect], withstand, recover, and evolve in order to improve their capabilities in face of adverse conditions, stress, or attacks to the cyber resources it needs to function'' [20]. Since this definition includes cybersecurity within the cyber resilience concept [24], cybersecurity will be considered part of cyber resilience from this point on. The adopted definition also defines the stages of the cyber resilience lifecycle: anticipate, detect, withstand, recover, and evolve (Figure 1).

The holistic nature of cyber resilience makes it multi-dimensional, and multi-disciplinary requiring several areas of knowledge to be involved [25], [26], [38]. These areas of knowledge or dimensions have several names in the literature (e.g. domains, categories, capabilities, controls, etc.). However, in this study the term ''domain'' has been adopted to refer to these categories, capabilities, controls, etc. since it is the name used in several other studies [20], [31], [39].

Moreover, these domains have several actions, or measures that SMEs can implement in order to implement the domain. These actions are, within the context of this article, called policies since in a generalized manner they represent concrete actions that the managers of the company would need to implement in order to operationalize cyber resilience.

Companies, however, and SMEs in particular, are propense to being reactive and protective (''fail-safe'' approach) [30] towards the implementation of cyber resilience. This makes them propense 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) [40]. 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'' [41]. Thus, companies not only require cyber resilience operationalization, but also need a systematic and proactive approach towards this operationalization because adding more protective measures does not always correlate with more security. Therefore, cybersecurity and cyber resilience frameworks can prove to be useful tools to make cyber resilience operationalization more systematic. The following subsections develops on the literature's current cyber resilience frameworks and the need for an SME approach.

A. RESEARCH GAP IDENTIFICATION

Despite the need for implementing cyber resilience in companies and especially SMEs, these organizations still commonly underinvest in its policies because of their lack of awareness about its implications [14], [30]. Besides, SMEs' usually do not have enough means to invest in the required protection, leaving significant risk uncovered [8]. This combination of a lack of awareness and lack of resources make cyber resilience difficult to implement since not being aware is also a cause for not investing or underinvesting [42].

Due to this difficulty of implementation several frameworks, standards, methodologies, maturity models, and assessment tools have proliferated in the literature. Some examples of these can be found in the following references: [20], [23], [25], [27], [31], [32], [39].

A literature review on cyber resilience frameworks 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 paper 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 paper 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. 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 paper'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.

After searching and applying the criteria, 18 frameworks were selected and analyzed. Table 1 shows a list of the 18 identified frameworks that matched these criteria.

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

1. Audience: 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: 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 2, 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.
1. Lifecycle: 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 [21]. In this sense, the document is assigned a ''yes'' in Table 2 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

TABLE 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 [43]
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 [44].
3	2012	Information Systems Audit and Control Association (ISACA)	A Business Framework for the Governance and Management of Enterprise IT COBIT 5 [45]
4	2012	Hong Kong Monetary Authority	Cyber Resilience Assessment Framework [46]
5	2012	MITRE Corporation	Cyber Resiliency Metrics [23]
6	2013	Linkov, I. et al.	Resilience Metrics for Cyber Systems [27]
7	2013	International Organization for Standardizations (ISO)	ISO/IEC 27001:2013 [47]
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) [32]
9	2014	Department of Energy (DOE)	Cybersecurity Capability Maturity Model (C2M2) [31]
10	2016	Carnegie Mellon University	Cyber Resilience Review [39]
11	2016	World Economic Forum (WEF)	A Framework for Assessing Cyber Resilience [28]
12	2016	Carnegie Mellon University	CERT Resilience Management Model (RMM), Version 1.2 [48]
13	2016	Nys, J.	How to Steer Cyber Security with Only One KPI: The Cyber Risk Resilience [38]
14	2017	World Economic Forum (WEF)	Advancing Cyber Resilience: Principles and Tools for Boards [49]
15	2018	National Institute of Standards and Technology (NIST)	Framework for Improving Critical Infrastructure Cybersecurity v 1.1 (NIST Cyber Security Framework) [25]
16	2019	Center of Internet Security (CIS)	CIS Controls V7.1 [26]
17	2019	Pacific Northwest National Laboratory	Buildings Cybersecurity Capability Maturity Model (BC2M2) [50]
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] [20]

TABLE 2. Comparison of cyber resilience frameworks.

Nº	Audience	Profiling	Lifecycle	Focus	External aspects	Implementation order
1	Companies	No	No	Information Security and risk management	No	Yes
2	Companies	Yes	Yes	Risk management and vulnerability management	No	No
3	Companies	Yes	No	Governance of IT and risk management	Yes	Yes
4	Banks	Yes	Yes	General	Yes	No
5	Companies	Yes	Yes	General	No	No
6	Federal agencies and Companies	No	Yes	General	Yes	No
7	Companies	Yes	Yes	Information Security and risk management	Yes	No
8	Federal agencies and Companies	Yes	Yes	General	No	No
9	Companies	No	Yes	General	Yes	No
10	Companies	No	No	General	Yes	No
11	Companies	No	Yes	General	Yes	No
12	Companies	Yes	Yes	General	Yes	No
13	Companies	No	No	General	No	No
14	Companies	No	No	Governance and risk management	Yes	No
15	Critical Infrastructures	Yes	Yes	General	Yes	No
16	Companies	No	Yes	General	No	Yes
17	Companies	No	Yes	General	Yes	No
18	Companies	No	Yes	General	Yes	No

the importance of preparing and becoming safe-to-fail instead of trying to be fail-safe.

2. Focus: 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.
3. External aspects: 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.
4. Implementation order: This property refers to whether the framework suggests an order in which the policies it defines have to be implemented. In this sense, the document is assigned a "yes" in Table 2 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.

Table 2 shows there are no frameworks that match all of these ideal properties for a cyber resilience framework for SMEs. This means there is no framework targeted for SMEs to use as it is (without requiring 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 an implementation order. Although individually these characteristics are highly adopted by cyber resilience frameworks, as a group they are not present in any of the analyzed frameworks.

Moreover, SMEs need a cyber resilience approach that fits these characteristics because without it, in the current threat scenario, they risk going out of business and being targeted [6]–[8]. For bigger companies, cyber incidents could also be a big problem, but they would not be as propense to going out of business for a cyber incident as SMEs are. In addition, bigger companies might be able to implement cyber resilience policies through consulting projects or big internal projects that would not be possible for SMEs to finance. Instead, SMEs require a systematic approach that builds cyber resilience through a distribution of resources over time, otherwise, they would not be able to implement these domains and policies. Therefore, this study claims that a cyber resilience framework that includes implementation guidelines such as an implementation order to suit SME needs is required. For this reason, this article aims to develop a framework with those characteristics.

III. METHODOLOGY

In order to obtain the framework and help SMEs operationalize cyber resilience, a variation of the design science research (DSR) methodology has been used. DSR methodology is used in this article 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.) [51]–[55]. 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 has been used to identify common essential concepts among the cyber resilience frameworks. Grounded theory is useful for this purpose since it is a methodology designed to extract concepts out of empirical data [56]. In this case this methodology is used to define a framework for SMEs, similar to the way it is used in other studies to extract essential concepts [57]. Moreover, after the usage of the grounded theory methodology, this process included the participation of 11 experts. Six experts participated in an iterative process in which through inputs from the literature and the experts' feedback, the framework improved during four iterations. During these experts' feedback sessions, the framework's domains 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.

Finally, semi structured interviews with a set of 5 experts were used to validate the adequacy of the framework to qualitatively evaluate their usefulness in the specific scenario of SMEs.

Figure 2 summarizes the followed methodology. Each stage of the methodology is explained in the following subsections.

A. GROUNDED THEORY

Grounded Theory methodology aims to find new theories from the iterative process of coding and comparing the concepts in the data [58]. 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 [56]. Many grounded theory analysis are based in document analysis [57], [59] 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 [57]–[59]. 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 [58].

In this study, the documents used to start the grounded theory analysis were the 18 frameworks identified in the literature review from the previous section.

On the other hand, 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 [60]. Similar combinations of coding techniques within the grounded theory methodology are commonly used, and encouraged by other authors [57], [60], [61].

The open coding approach was used to assign codes, compare, conceptualize, and categorize the available data [60], [62], [63]. In this case, the available data was the policies, domains and concepts in the cyber resilience frameworks. For this reason, the frameworks 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 [60], [64]. 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 [31], [39]. However, these domains would be equivalent to what is found as ''categories'', ''capabilities'' or ''controls'' in other frameworks [25], [26], [38].

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, the cyber resilience framework contained 10 domains and 32 policies in total.

B. ITERATIVE DEVELOPMENT

After a result was reached from the Grounded Theory methodology, six experts participated in an iterative reviewing process. The six experts had wide experience in cyber

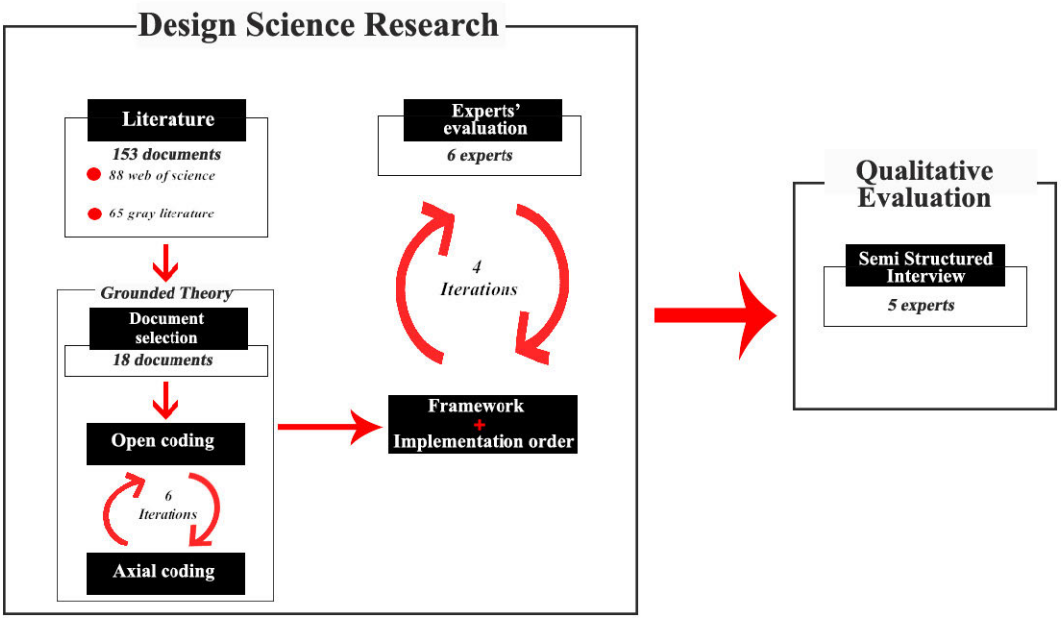

FIGURE 2. Methodology diagram.

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 domains 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.

C. QUALITATIVE EVALUATION

To evaluate the usefulness of the framework (including its implementation guidelines) developed in the previous steps of this methodology, five experts participated in semi-structured interviews. 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 defined with the literature and the feedback of the previous 6 experts and asked several questions 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?".

IV. CYBER RESILIENCE FRAMEWORK FOR SMEs

After applying the methodology described in the previous section, cyber resilience has been synthesized into 10 domains and 32 policies for SMEs to follow and implement. As mentioned in the previous section, the policies and domains in this 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 framework and a comparison to other frameworks in the literature is given in Table 3.

A. GOVERNANCE

The reviewed cyber resilience frameworks often reference concepts related to the role of the management in promoting/sponsoring cyber resilience [31], [39], [43], [45], [46], [49], [50], communicating cyber resilience plans [27], [28], [39], [50], developing a cyber resilience strategy [25], [31], [38], [45], [49], [50], assigning enough resources to develop

cyber resilience activities [43], [46], [50], and complying with cyber resilience-related regulation [28], [38], [45], [47], [48]. The framework has grouped this common theme under one domain called ''governance'' since several of these frameworks explicitly name similar groups under that name [25], [38], [39], [46].

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 [18].

Governance is key for the anticipation stage of the cyber resilience lifecycle since it is where the company's management decides where to put their efforts [18]. However, due to the importance of governance in the implementation of other cyber resilience domains that are explained in the following subsections it can indirectly influence the detect, withstand, recover, and evolve stages of the lifecycle.

Due to the characteristics of the governance domains, it is important for every company, including SMEs, to implement the policies in this domain, but especially to have cyber resilience promoted by the strategic management to the company.

B. 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 [25], [31], [39], [43], [46]–[50], the classification of these risks in order to determine priorities [25], [26], [31], [39], [47], [48], [50], the determination of an acceptance threshold for risk [25], [31], [39], [46], [48], [49], and the development of risk mitigation activities [25], [31], [32], [39], [43], [47]–[50]. In this article's framework, 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 [25], [31], [32], [38], [39], [43], [46]–[50].

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 [25], [31], [39]. 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 [21].

Risk management directly affects the anticipation and detection stages of the cyber resilience lifecycle since it is in the risk management where the company gets information on the risks they might face [43], [49]. This knowledge can help them put the appropriate measures to be prepared for known risks and detect when those risks have been exploited.

In order to effectively operationalize cyber resilience, SMEs must start by addressing known risks. It is important for SMEs to prioritize these risks and address the most impactful and the most propense to happen. The investment in this domain and its policies would help them avoid future incidents from these known risks and thus, in most cases, avoid them going out of business for this [6].

C. 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 [20], [25], [26], [31], [32], [39], [46]–[48], [50], creating and documenting a baseline configuration of the assets and a configuration change policy [25], [26], [31], [32], [39], [48], keeping the assets maintained [20], [26], [31], [32], [39], [46]–[48], and identifying the internal and external dependencies of those assets [27], [28], [39], [46], [48]. The name of the domain that groups these concepts in this article's framework is ''asset management'' because it is a name commonly used to group these concepts together in the reviewed frameworks [25], [39], [48], [50].

Based on these concepts and the experts' input, the asset management domain of the framework for this article 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 [27].

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 [21], [42].

In order for SMEs to protect themselves, SMEs need to know what they have and what could be affected in case of a compromised asset. Thus, experts agreed that it is important to implement the asset management policies for the SMEs to be aware of what they have to protect. Moreover, in order to avoid unintended side effects of configuration changing, the experts considered necessary to keep track of the base configuration and the history of changes in order to be able to revert to previous configurations, or to identify the cause of a certain unwanted behavior of the assets.

D. 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 [23], [27], [28], [31], [32], [38], [39], [43], [44], [46], [50] and mitigating the company's threats and vulnerabilities [23], [31], [38], [39], [43], [44], [48], [50]. 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 [31], [38], [39], [47], [50].

Due to these common concepts and after iterating with the experts, the cyber resilience framework for SMEs 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.

According to the experts, threat and vulnerability management contributes to the anticipation and detection stages of the cyber resilience lifecycle. In this sense, identifying and mitigating threats and vulnerabilities help companies be more prepared against incidents, and knowing the threats and vulnerabilities that cannot be extinguished can help companies set detection methods in case these are exploited.

E. 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 [20], [25], [27], [28], [39], [46], [47], determining the causes, objectives, points of entry and methods that enabled the incident [25], [27], [28], [38], [39], [46], [47], [50], and analyzing the responses and response selection process after an incident occurred [25], [27], [28]. These concepts are often mixed with the response to incidents under an incident management domain or similar [20], [25], [26], [38], [39], [46]–[48], [50]. 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 [25], [27], [28], [32], [39], [47], [48], 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 cyber resilience framework for SMEs 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.

The experts have agreed that incident analysis can help in all of the cyber resilience lifecycle. They argued that knowing what has happened in the past lets you improve for the future (evolve), know how to resist the same incident in another instance (withstand), know what to do in order to recover from it (recover) and prepare so that it does not happen again (anticipate and detect).

F. AWARENESS AND TRAINING

Another recurrent theme in the reviewed frameworks that the experts considered important for a cyber resilience framework for SMEs 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 [26], [31], [32], [48], making sure the company's employees had the adequate training for their roles in the cyber resilience strategy [20], [23], [25], [26], [31], [32], [44], [47], [48], [50], raising the company's employees' awareness [25]–[28], [31], [32], [47], [48], and training the personnel in technical skills [20], [23], [26], [31], [32], [45], [47], [48], [50]. These concepts have been grouped under the ''awareness and training'' domain, because the title is used in several of the reviewed frameworks [25], [26], [32], [38], [39], [48].

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.

According to the experts, awareness and training is another domain that affects the whole cyber resilience lifecycle. It is important for the management and the employees to be aware

and well trained in order to anticipate, detect, withstand, recover, and evolve [18], [22].

To make implementation of other domains cost effective, training is a very important domain. This domain can help companies avoid social engineering attacks and can help companies perform better in other domains. Thus, to make cyber resilience implementation as cost effective as possible for SMEs, this domain and its policies are necessary.

G. 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 framework 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 [23], [25], [31], [32], [38], [39], [44], [47], [48], [50]. Protecting the integrity through integrity checking mechanisms in data, hardware, software, and firmware [23], [25], [26], [31], [32], [39], [44], [47], [48]. Finally, protecting availability through back-ups, redundancy and maintaining adequate capacity [23], [25], [28], [31], [32], [39], [44], [47], [48]. The protection of the CIA triad is often called ''information security'' [47], 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.

Information security mainly affects the anticipate and withstand stages of the cyber resilience lifecycle. According to the experts this is because information security measures are mainly used as protection which is preparation for known threats [24], and to withstand in case those threats are exploited.

The use of information security is crucial for SMEs to mitigate their risks and try to avoid cyber incidents as much as possible since these could potentially leave them out of business [6]. Thus, although the investment in these policies may be expensive, it is necessary for the mitigation of the most important risks.

H. 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. [20], [23], [25]–[28], [31], [32], [38], [39], [44], [47], [48], [50]. 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 [20], [25]–[27], [39], [46], [48], [50]. These concepts are often found in the reviewed frameworks as ''continuous monitoring'' or similar [20], [25], [32], [48], however, to emphasize the objective of the monitoring, this article uses ''detection processes and continuous monitoring'' as the title that encompasses this group of concepts. The ''detection process'' is inspired by [25] 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.

According to the experts, the detection processes and continuous monitoring domain contributes to the cyber resilience lifecycle in the stages of anticipate, detect, and withstand. Their reasoning was that monitoring, and detection help prevent (anticipate) incidents, the monitoring and detection processes are there to detect incidents in case of occurrence, and detecting an incident early can be an important factor in resisting the incident (withstand).

I. 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 [20], [25], [31], [32], [39], [44]–[48], [50], to determine actions and responsibilities in order to recover normal operations and define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) [20], [23], [25]–[28], [31], [32], [38], [39], [44], [46]–[48], [50], and to test these business continuity plans periodically to determine their effectiveness and adjust them accordingly [20], [25], [26], [31], [39], [44], [46]–[48], [50]. 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 [20], [32], [44], [47], [48] 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 cyber resilience framework for SMEs 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.

Business continuity management mainly affects the stages of withstand, recover and evolve in the cyber resilience lifecycle. These plans are defined in order to resist the incidents as much as possible with operations as normal as possible (withstand), recover the normal operations as quickly as possible (recover), and learn from these experiences after the events (evolve) [25], [39].

As mentioned before, SMEs are propense to having to stop their activity and have such high costs due to cyber incidents that many of them go out of business due to cyber incidents. Thus, it is important for them to define plans of action in which they could work despite adverse situations. This could potentially help SMEs survive during and after an incident.

J. 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 [20], [25], [27], [28], [31], [39], [49], [50], 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 [20], [25], [31], [45], [50], and collaborating with the company's suppliers and third party partners to implement the appropriate measures to meet the company's cyber resilience needs [25], [31], [32], [44], [45], [47]–[50]. 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 [20], [31], [49], [50] and it was considered the most appropriate by the experts.

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.

The information security and communication domain is important for cyber resilience because it represents one of the biggest expressions of the ''network of organizations'' approach that differentiates cyber resilience from the ''one organization'' approach usually adopted in cyber security [21]. It is this domain's purpose that the company collaborates with external entities including public and private organizations that surround them.

After describing the 10 domains and its policies' origin, Table 3 presents a summary of the domains, policies and the references that include them. The contents of Table 3 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.

Finally, the information security 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 [42].

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 framework, thus reducing the necessary resources for the implementation.

V. IMPLEMENTATION ORDER DEFINITION

Other frameworks existing in the literature help companies identify policies and actions needed to operationalize cyber resilience. However, only a few of them define some kind of order in which these actions policies have to be implemented. On the other hand, in the discussions with experts, they considered that the policies' implementation order could influence their effectiveness. 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. In turn, an incident that affects an unprotected critical asset could represent high costs [5], [65], [66] and a company that has invested considerably

TABLE 3. Cyber resilience framework for SMEs and other frameworks influences.

		Reference to analyzed documents with indexes from Table I																	
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			

in protecting other assets could lead to the assumption that "spending" in cyber resilience is not effective.

A. CURRENT IMPLEMENTATION ORDER

Before discussing an order of implementation, the experts were asked what was, in their experience, the cyber resilience domains' implementation order companies follow today. To answer this question the experts quickly agreed that today companies are used to the traditional cybersecurity approach where humans are kept out of the equation as much as possible and technology is key for protection and detection [29], [30]. In this sense, the experts agreed that, following the nomenclature of the framework, the companies usually do the following: They first implement the domains that can be implemented through technological tools such as

TABLE 3. *(Continued.)* **Cyber resilience framework for SMEs and other frameworks influences.**

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	

information security, **detection processes and continuous monitoring**, **threat and vulnerability management**, and **asset management** because they argued that these can be implemented by using products that are common in the market and thus are the most popular measures and the easiest to implement. This is consistent with the idea that traditional cybersecurity is mainly technological [29], [30].

Then, according to the experts, **risk management** comes almost as a result of implementing these technological tools and becoming concerned about the possible cyber risks. From the experts' point of view, this is usually where companies stop their cyber resilience implementation, which is about the boundary between cybersecurity and cyber resilience. This is consistent with the literature since studies show that this is a false sense of security derived from feeling protected against known threats [19], [67].

However, the experts stated that after an incident occurs, the rest of domains start to become a concern. This reasoning is similar to the raise in the management's awareness after an incident found in other studies [67]. In addition, after an incident, the company starts to investigate what happened and why (**incident analysis domain**). The company's management start to get more involved because of the concern and may start to promote strategies, implementing a part of the **governance** domain. Then, the management wants the company to be more prepared in case something happens again, so they start to implement **business continuity management**, and they start to raise awareness and train the personnel (**awareness and training**). Finally, the companies that become more mature after this process start to implement **information sharing and communication** to learn from others how to improve in the other cyber resilience domains and thus be more resilient. Figure 3 depicts the current implementation according to the experts as described before.

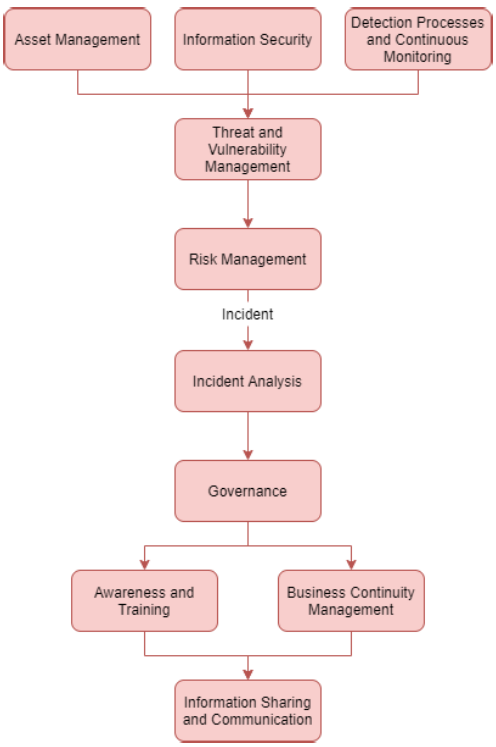

FIGURE 3. **Current Cyber Resilience Domain Implementation Order.**

On the other hand, the experts discussed that this order could be inefficient for companies. The literature suggests, for instance, that installing detection systems in a company

where the personnel in charge of it does not have enough experience could be counterproductive because they would not handle false alerts correctly [68].

B. EXPERTS' OPINIONS AND BACKGROUND DIFFERENCES

Once they had established a clear basis on how companies currently implement cyber resilience, the experts were asked to give their opinion on how the current implementation order should be improved to be more effective for SMEs. The experts discussed their thoughts and experience on a way to implement cyber resilience during 4 iterations. During these discussions, it was obvious that the background of the experts influenced the way they ordered the domains of the proposed framework.

The two experts with a more technical background argued that the first actions should be towards an effective technological implementation. In this sense, they argued that the first steps towards cyber resilience should be the steps towards a good risk management informed by the information of the company's assets (**asset management**), analysis of previous incidents (**incident analysis**), and threats and vulnerabilities' repositories (**threat and vulnerability management**). A well-informed **risk management** would let the company implement the necessary measures to protect against known threats (**information security**) and implement measures to detect incidents related to these threats (**detection processes and continuous monitoring**). According to them, after implementing these technological measures is when the management should start to get more involved (**governance**). The management should promote the planning for contingencies (**business continuity management**) and the **training and awareness** of all the personnel in order to avoid incidents due to human mistakes and to be prepared in case of an incident. The final domain to implement according to the experts in this background was the **information sharing and communication** which they saw as an opportunity to build further cyber resilience after they have achieved certain maturity in the internal aspects of cyber resilience. Figure 4 depicts the implementation order described above.

On the other hand, the 4 experts with a more strategical background suggested that cyber resilience must be the initiative of the management (**governance**). The management should be the one that strategizes what to protect, how, and with how much resources. The experts argued that the management would naturally be concerned with business continuity, so the next steps were towards an early business continuity management. In this sense, the second domain that should be implemented according to them was **asset management** to know what is it that the management wants to protect the most. They argued that the personnel had to be trained and be aware in order to implement any of the following domains, so **training and awareness** was the third domain for them. After this, the company should start to analyze the most important risks (**risk management**) and plan for how to maintain operations despite the exploitation of one

FIGURE 4. Initial Implementation Order for Experts with Technical Background.

of those risks in the company (**business continuity management**). After implementing these domains, the experts with this background considered it was the moment to start protecting the company's assets by implementing **information security**, **detection processes and continuous monitoring**, **threat and vulnerability management** and **incident analysis**. According to the experts, these four domains should be implemented to mitigate risks identified in the risk management domain and in this way avoid as much as possible having to need the business continuity plans (avoid having incidents). Finally, and similar to the experts with a more technical background, the experts in this group considered that the last domain was **information sharing and communication**. They argued that it is important to cooperate, but that to cooperate with others it is important to have a solid base. Figure 5 shows the implementation order that experts from this background suggested.

C. CONSENSUS ON AN IMPLEMENTATION ORDER

After discussion and 4 iterations, the experts reached a compromise establishing the following domain implementation order as a viable approach for SMEs: the first thing that a company should seek when implementing cyber resilience is to define a strategy. This will help them achieve their goals in a much more effective way since the cyber resilience strategy will let them know what the company needs to protect and how. The literature also shows that today's context makes

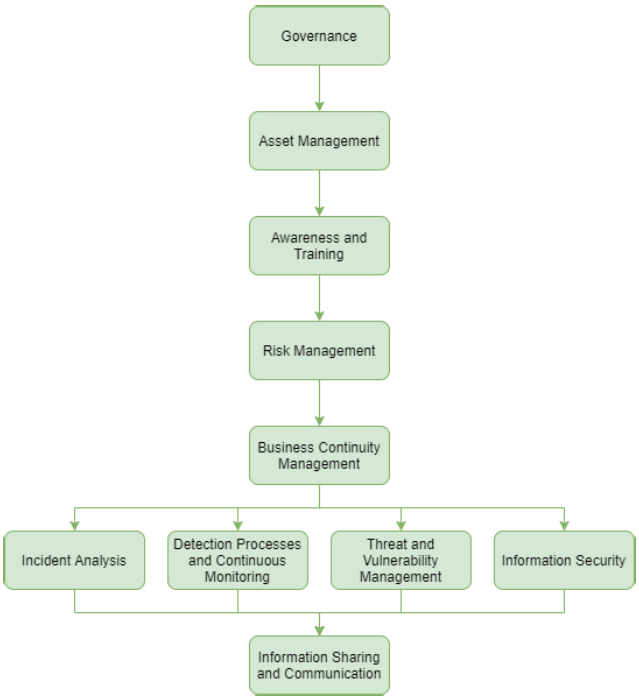

FIGURE 5. Initial Implementation Order for Experts with Strategical Background.

strategy from the management more important than ever [18]. This is why the **governance** domain should be the first goal for the companies. However, it is not possible to establish a strategy that defines the security policies, the company's priorities, and the needed measures, without knowing what risks and types of risks the company is exposed to, and thus, an exhaustive and well-done **risk management** should be done in order to define an effective strategy against those risks.

Each of the assets that the company has could potentially be attached to specific risks, especially the technological assets. For this reason, in order to do an effective risk management, companies must first know what they have inside their companies, which of those assets are critical for their business, and thus, they must implement the **asset management** domain. After implementing the asset management domain, companies must be aware of the threats and vulnerabilities that their assets are exposed to. This means they should implement the **threat and vulnerability management** domain. The threats and vulnerabilities identified in this domain will also help feed the risk management processes.

To aid the threat and vulnerability management, the company must include the analysis of what has happened previously and why. Thus, the company has to feed the threat and vulnerability management with the **incident analysis** domain. The combination of asset management, incident analysis, and threat and vulnerability management resulting in an effective risk management is also backed up by the literature [43], [44].

After using these tools to develop a good cyber resilience strategy, the company should start to think how they could react in order to maintain their business running despite the identified possible incidents and prepare for the situation in which an unexpected incident occurs. This requires the company to implement the **business continuity management** domain.

Besides finding ways to keep the operations running despite the occurrence of an incident and now that the company has a defined strategy, the company needs to implement traditional cybersecurity measures. This means that the company needs to find ways to detect incidents as early as possible and be as effective as possible when reacting to these incidents. To achieve this, the company needs to define monitoring techniques for the critical assets and define a detection process. This requires the company to implement the **detection processes and continuous monitoring** domain. At the same time, the company should implement good **information security** techniques in order to protect these assets. According to the experts, solutions that protect the company's information security are very often technological and/or part of a good configuration of the systems in the company. However, companies should try to keep in mind the information security principles in every way, including the physical security.

The experts also emphasized that the last three domains (i.e. business continuity planning, detection processes and continuous monitoring, and information security) will also be fed by the incident analysis domain, because the past incidents will also help determine what happens when the company suffers an incident. This knowledge could help determine how to protect against the past incidents, detect them and keep operations going despite them.

With all this in place, the company can start to cooperate with other entities and share information to learn about the best practices, threat trends, new vulnerabilities, more effective ways of protecting, etc. This means, they should put efforts in implementing the **information sharing and communication domain** to transfer and receive useful information that will help improve the company's cyber resilience. This domain too, should be improved with the practice of the incident analysis in order to share the best possible information and receive better information about what has happened to the company and how to be more resilient towards it.

Finally, every domain mentioned in the framework has to be supported by the **awareness and training**domain. This is because every aspect of cyber resilience requires the company's management to be aware of the threat landscape, and the personnel to be aware of the need for cyber resilience and trained to perform the actions required to implement each of the other domains in the best way possible. The literature also emphasizes the importance of awareness and training to be the base of other domains such as governance [18], or detection processes and continuous monitoring [68].

The order of implementation according to the consensus of the experts is depicted in Figure 6.

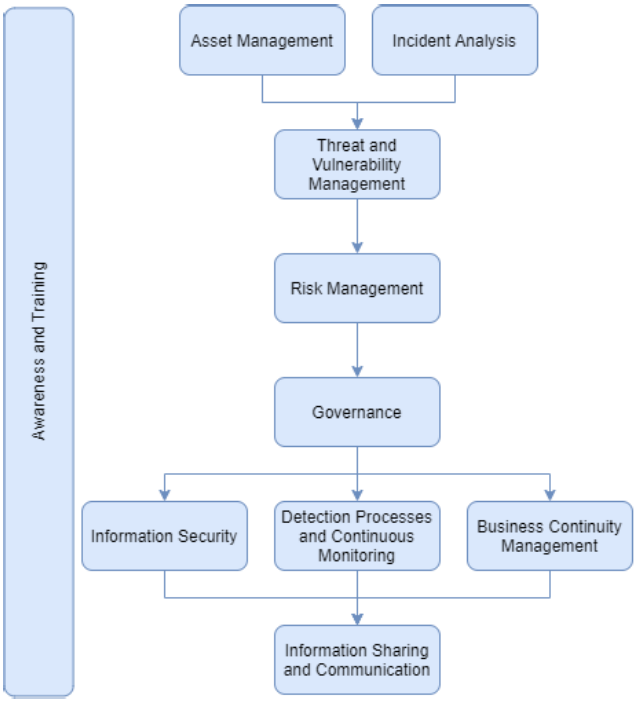

FIGURE 6. Cyber Resilience Framework's Implementation Order.

VI. FRAMEWORK APPLICATION

The presented framework is intended to aid companies in the process of deciding which cyber resilience policies to implement and a suggested order. Moreover, the implementation of the cyber resilience domains in the order specified in the implementation order is intended to make the operationalization of cyber resilience as attainable and comprehensive as possible because the implementation of the policies from the first domains would be the base of the implementation for the rest.

However, the implementation of the policies can still require considerable investment which could still be a problem for SMEs. This is especially true since the policies in the presented framework can be interpreted from different maturity states of cyber resilience implementation. For instance, making an inventory and a classification of the company's assets can be interpreted as: a) A list of the company's assets with the identification of the most critical assets for the business, or b) a list of the assets with their physical and network location, that is updated through a defined protocol and that has a scoring system or objective criteria for determining criticality [25].

In order for SMEs to implement these policies, it cannot be done at the highest maturity state from the beginning. It would also be impossible for SMEs to implement all the policies at once since it would require unreasonable amounts of resources. Instead, in order to reduce the investment, it is suggested that they do it through a stepwise refinement process. In this kind of process, the policies would be implemented at a certain level of maturity, but the implementation would be, in a future iteration, improved upon.

Another important observation is that the implementation of the framework's policies does not necessarily need to be done by the company itself. In some cases, for cost efficiency, it might be a good option to outsource the implementation of some cyber resilience policies. As argued in previous sections, cyber resilience policies require specialized knowledge to implement. For instance, implementing network segmentation can be complex and most current techniques depend on manual configurations in which many companies make mistakes [69]. Hiring a third party to implement some of these cyber resilience policies can help the company implement cyber resilience policies without previously acquiring that specialized knowledge, and thus also reduce the time needed to implement the policies.

The following subsections elaborate on both ideas, the use of a stepwise refinement process and the use of outsourcing. Notice that these two ideas are separated for clarity purposes but can be combined in practice.

A. STEPWISE REFINEMENT PROCESS

Stepwise refinement is a software development paradigm in which a complex problem is broken down into simpler, well-defined tasks that are developed and later added to solve the more complex problem [70]. This methodology has helped software engineers conceptualize and add functionality gradually to meet the requirements of clients in a more effective manner [71].

In analogy, this kind of methodology can help SMEs implement cyber resilience policies effectively through iterative steps in which the investment is distributed into smaller implementations, this would also help the SME acquire knowledge from experience of previous implementations to improve upon the following iterations.

To use the combination of the framework and this methodology, companies can use the following process:

1. Choose some policies from the framework taking into account their domain and the order of implementation suggested by the implementation order, their capabilities, and the available budget.
2. Define the objective implementation state of those policies' implementation after an iteration of the methodology that fits the available budget, and the company's capabilities.
3. Evaluate whether these objectives can be achieved with the internal resources or if they would be better implemented through outsourcing by checking the criteria in the next subsection of this article.
4. Implement the selected policies.
5. Evaluate the implementation of the policies and compare to the objectives set in step 2.
6. Repeat the process.

This process also aligns with the philosophy of continuous improvement. In continuous improvement, the

Plan-Do-Check-Act (PDCA) cycle is commonly used to implement lean thinking, quality control and other concepts [72]. The proposed process does not have to be followed continuously (which would require high investments) but can be directly compared to the iterative way in which the PDCA cycle is used.

Stepwise refinement, iterative continuous improvement and agile development methodologies, such as incremental development [73], all help achieve complex tasks more effectively [70], [72], [73]. Moreover, they all require a modularized implementation in which the cost and understanding of each iteration should be lower than in a complete implementation thus making each investment easier to justify and easier for less knowledgeable companies, such as SMEs, to implement. Thus, the idea behind these methodologies can be applied in the field of cyber resilience to achieve effective implementation through smaller, iterative investments.

B. OUTSOURCING

As mentioned above, outsourcing can ease the implementation of policies in which specialized knowledge is required, such as network segmentation [69]. Despite this being convenient, outsourcing is not cheap and, on the contrary, it sometimes requires considerable investment. However, by following certain criteria, it can be used to help the company operationalize cyber resilience policies effectively in less time [74], [75].

A good practice in this sense would be to follow objective criteria such as the criteria that would be used to outsource any kind of IT management. This is a highly studied problem in the literature and would include to consider and evaluate strategy, organizational characteristics, economic and contractual factors, and technological benefits of outsourcing to objectively make a decision of whether to outsource or to centralize the implementation of a policy [76]–[79].

In this case, in which the objective of outsourcing would be to achieve effective implementation of cyber resilience policies, this article presents three common reasons for which companies use outsourcing:

1. Cost. Outsourcing is commonly used when the cost for implementing an iteration of a cyber resilience policy would be too high compared to the implementation by a cyber resilience provider.
2. Availability. The next reason would be if the company does not have the personnel with the expertise or if the personnel with the expertise in the company does not have the availability to implement the policy.
3. Time. Outsourcing can also be useful when the time required to implement an iteration of a cyber resilience policy with the company's resources would be too high and unreliable compared to the implementation by a cyber resilience provider.

To illustrate these criteria, the next three subsections will give an example of each of these cases.

1) OUTSOURCING FOR COST EXAMPLE

A theoretical example of outsourcing for cost in cyber resilience implementation would be a small business that wants to improve their detection and continuous monitoring. To do so, would mean to buy the needed commercial tools such as an Intrusion Detection System (IDS) and a Security Information and Event Management (SIEM) and train the personnel to use these tools. However, this kind of project is provided by cyber resilience providers and can be outsourced. Outsourcing this implementation will save the costs of buying the tools and training the personnel and thus potentially save costs for the company.

2) OUTSOURCING FOR AVAILABILITY EXAMPLE

An example of outsourcing for availability could be a small industrial company that provides parts for an automobile factory wants to secure communications between their machines through information security techniques. They would want to do so in order to avoid sabotage, espionage, leaks of intellectual property or even denial of service attacks, all of which would lead to problems with their clients. Their problem, most times would be that they do not have the expertise to implement these measures. In order to focus on the core of their business (the production of the parts for the automobile factory), it would be a good decision to outsource the implementation of these information security measures. This way, the company can potentially save resources since they do not have to hire new specialized personnel or hire new personnel and send them to a specialized training.

3) OUTSOURCING FOR TIME EXAMPLE

A hypothetical example of outsourcing for time in cyber resilience implementation would be a business who wants to make a threat and vulnerability analysis of their systems. If they do have the personnel, but do not have the tools nor the knowledge to do so, the use of outsourcing would be a faster way of achieving the implementation of these policies. Since this is an automatic process, one person with training and the correct tools should be able to do this faster than the company who has to find the tools, and maybe even train a person to do the analysis.

VII. QUALITATIVE EVALUATION OF USEFULNESS

As mentioned in previous sections, the framework was developed with the contribution and iterative feedback from 6 experts. The remaining 5 experts were interviewed in order to qualitatively evaluate the adequacy, viability and usefulness of the framework. These 5 experts were presented with the framework without any background on how it was developed and asked to read carefully and do a face validation. They were also asked to try to find missing information, give their thoughts on the implementation order based on their experience, and if needed to suggest changes. After this, they were specifically asked to consider an SME with low cyber resilience level and with almost no knowledge

about cyber resilience implementation and try to judge from that perspective if the information provided by the framework would be useful to get started with cyber resilience implementation.

The results from these interviews were the following:

- None of the experts thought that there were missing domains nor policies in each domain.
- Two out of the five experts thought that in the information security domain the dependencies can be very variable depending on the sector of the company. For instance, a hospital must prioritize confidentiality measures, but on the other hand, an industrial company would more likely prioritize maximizing availability. However, the experts recognized that for a general framework it is very difficult to reflect this. Therefore, to keep the framework as a useful starting point for all SMEs regardless of their sector, these policies were left as general guidelines for the company's managers to understand interrelationships between the domains and policies. However, in order to get into more a detailed, policy-level implementation, the company must adapt according to their needs and circumstances.
- When asked about the dependencies between the domains and the order of implementation one expert pointed out that although the dependencies are correct, in an implementation order the incident analysis domain will not always be possible to implement at the beginning for two reasons. The first is that the company must have suffered an incident previously and have collected information in order to analyze it. The second one is that it probably requires a higher maturity level in order to implement this domain. The implementation order, however, is meant to provide general guidelines for SMEs to understand the interrelationships between the cyber resilience domains. Thus, it depicts an ideal situation but in case the company does not have the ability to implement the domains in that order, it does not mean they are operationalizing cyber resilience in a wrong way, but rather, that their current situation requires a slightly different approach. As the expert said, in the best case scenario the dimensions should be implemented that way, but if the company has not suffered incidents or has not collected information from incidents, they should only take into account that they could do so in the future in order to improve their cyber resilience operationalization.
- Finally, as for the usefulness of the framework and implementation order, 4 out of the 5 experts considered this combination to be useful as it is. The fifth expert suggested that the results should be presented using a more pedagogical approach. Work in progress related to this comment is trying to adapt the concepts in the framework and implementation order into a more comprehensible tool for evaluating the company's current cyber resilience level and propose actions to improve upon the current level.

As shown by these results, the five experts who participated in the qualitative validation considered the framework and implementation order to be useful as guides to start to understand and operationalize cyber resilience. Although a few of opinions from these experts suggested certain nuances to the current version of the framework and implementation order, they all agreed that to a certain extent the combination of these results could potentially help SME managers understand the implications of cyber resilience and have clearer idea of the way to operationalize it in their company.

VIII. DISCUSSION

This article tries to combine the literature and the experience from cyber resilience experts to define a framework that is specific for SMEs. Thus, the results of this paper can be very useful for SMEs since, as argued in previous sections, they usually have limited specialized resources and knowledge about cyber resilience and using the synthesis presented in this article's framework can be more attainable than going into the fine print of cyber resilience as many other frameworks do.

Cyber resilience is a new approach that SMEs can have trouble to operationalize because of its holistic nature. The proposed cyber resilience framework for SMEs offers SMEs a synthesized but complete picture of what they need to build and operationalize cyber resilience, defining specific policies to build it, and a guideline on how to implement them.

Although each of the cyber resilience policies found in the proposed framework can be referenced to other frameworks, it is interesting to notice in Table 3 that there is no policy that exists in every framework. This means that there is a lack of consensus between frameworks about the important policies for each cyber resilience domain. This lack of consensus could represent another problem for SMEs because the decision of selecting the most appropriate cyber resilience framework could be left for chance or be another investment in time and resources in order to research the frameworks and select one.

In addition, Table 3 also shows there is no framework that contains all the policies that this article's framework does. This observation means that using any of the other cyber resilience frameworks individually could leave important information found in other frameworks behind. In practice, this could mean that the implementation of cyber resilience in that company is not as effective as it would be when using the cyber resilience framework for SMEs because it would lack some of the actions that are recurrent in many other cyber resilience frameworks.

The two observations that can be made from Table 3 are yet another reason why the cyber resilience framework for SMEs proposed in this article could be useful for SMEs. The implementation of this framework could be a starting point to ensure the implementation of the most important policies first.

This article also presents a cyber resilience implementation order that gives insight into the order in which cyber

resilience domains can be implemented in order to be effective. This result is also important for companies since it shows that cyber resilience has a completely different approach than cybersecurity. Cybersecurity has traditionally been started to be implemented through technology [29], [30], and other studies show that technology is really important at some points of the changing strategy to implement cyber resilience [67]. However, the experts and some of the literature [43], [49] agree that in order to implement cyber resilience effectively, the use of technology cannot be the first step. This means that the change in the approach will also mean that some of the companies' habits will have to change and few of the frameworks in the current literature offer guidelines on implementing their policies. The cyber resilience framework for SMEs, on the other hand, gains value due to the addition of the implementation order. This implementation order helps companies implement the framework's domains in an effective way by using the experience of experts as a basis. In turn, this means that the company will have concrete actions with a rough guide on what order they should be implemented and considering that the framework already captures the most important information from other frameworks in the literature, this implementation guidelines added to the framework become a combination that could help companies with less specialized resources and knowledge like SMEs [7], [10].

The methodology used to create this framework helps synthesize cyber resilience into its essential policies and domains. However, these are not the only policies that can be implemented in order to operationalize cyber resilience. In this framework several nuances have been omitted for the sake of simplicity and for SMEs to be able to have a general idea of how to operationalize cyber resilience. This can help SMEs better understand the implications of cyber resilience and leave SMEs on the correct path to continue their cyber resilience operationalization journey, but the lack of nuances and details will represent a handicap for the implementation of cyber resilience in companies that have the capacity and the resources to implement more advanced frameworks.

Thus, the framework must be treated as a guide and a starting point for their cyber resilience implementation. In many cases, the use of this combination can be used as presented in this paper, but companies should also consider if their situation may require changes to the order due to their circumstances. Although this might require a small investment to avoid naïve misuse of the framework, it can still guide companies in most of their implementation process. This can help companies with a limited knowledge base and specialized resources like SMEs [7], [10], [14], [15], [17].

IX. CONCLUSION

With the objective of aiding SMEs in the operationalization of cyber resilience, this article presents a framework that could potentially be used by SMEs to understand what domains and policies are implied in cyber resilience building process. In addition, the framework has been also presented in the form of an implementation order that SMEs can follow in order to operationalize cyber resilience based on experts' experience.

The usage of a Design Science Research approach in which Grounded Theory and iterative evaluations with an expert panel permitted the synthetization of cyber resilience into its essential dimensions, actions, and implementation order. This also allows the developed framework to be considered a starting point for cyber resilience building in companies, especially the ones with lower maturity level, such as SMEs.

In this sense, the main idea of the framework is not to be as specific and exhaustive as possible, but to be synthesized and generalist for SMEs to be able to understand what cyber resilience implies and start implementing it without being overwhelmed. This characteristic however, trades-off with the fact that companies with higher maturity levels should be aware that the framework in this article is to be considered a starting point and not an exhaustive guideline for cyber resilience operationalization.

Therefore, the use of the framework and implementation order could help SME managers in the process of cyber resilience building by giving them a synthetic tool with the essential actions and an order in which to implement them. This could help them start the cyber resilience operationalization process in an effective way whilst the use of other tools, that are more complex, would require them to select the actions that suit their needs and decide the order in which they should be implemented which in turn requires extensive knowledge, maturity and awareness. Thus, this could address the lack of specialized knowledge that SMEs have when starting to operationalize cyber resilience.

The results presented in this study can be useful for SMEs but are still limited to a theoretical approach with only a qualitative evaluation of the usefulness of the results. Thus, this article should pave the way for future lines of research wherein these theoretical tools are subject to test in real SME environments in order to reaffirm their validity and their applicability.

REFERENCES

[1] World Economic Forum, Geneva, Switzerland, 13th edition. *The Global Risks Report 2018*. [Online]. Available: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

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

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

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

[5] D. Tofan, T. Nikolakopoulos, and E. Darra. (2016). 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. [Online]. Available: https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/

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

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

[8] P. Millaire, A. Sathe, and P. Thielen. (2017). What all cyber criminals know: Small & midsize businesses with little or no cybersecurity are ideal targets. Trenton, NJ, USA. [Online]. Available: https://www.chubb.com/us-en/_assets/doc/17010201-cyber-for-small_midsize-businesses-10.17.pdf

[9] ENISA, Athens, Greece. (2015). *Information Security and Privacy Standards for SMEs*. [Online]. Available: https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport

[10] P. A. H. Williams and R. J. Manheke, "Small business—A cyber resilience vulnerability," in *Proc. Int. Cyber Resilience Conf.*, Perth, WA, Australia, Aug. 2010, pp. 112–117. [Online]. Available: https://pdfs.semanticscholar.org/a7b7/5c2c8d4400882be95dc68d2460739780facb.pdf

[11] M. A. Islam, M. A. Khan, A. Z. M. Obaidullah, and M. S. Alam, "Effect of entrepreneur and firm characteristics on the business success of small and medium enterprises (SMEs) in Bangladesh," *Int. J. Bus. Manage.*, vol. 6, no. 3, p. 289, Feb. 2011, doi: 10.5539/ijbm.v6n3p289.

[12] T. Mazzarol, T. Volery, N. Doss, and V. Thein, "Factors influencing small business start-ups: A comparison with previous research," *Int. J. Entrepreneurial Behav. Res.*, vol. 5, no. 2, pp. 48–63, Apr. 1999, doi: 10.1108/13552559910274499.

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

[14] T. Huelsman and S. Peasley. (2016). Cyber risk in advanced manufacturing. Richmond, VA, USA. [Online]. Available: https://www.nist.gov/sites/default/files/documents/2016/12/28/cyberrisk_manu_fullstudy_landscape _brochure_lpxcic07_06_17_7101_finalfor.pdf

[15] 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, Jun. 2016, doi: 10.1016/j.dss.2016.02.012.

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

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

[18] P. Binwal. (2015). Creating a cybersecurity governance framework: The necessity of time. Security Intelligence. Accessed: Dec. 17, 2019. [Online]. Available: https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time/

[19] H. Goldman, R. McQuaid, and J. Picciotto, "Cyber resilience for mission assurance," in *Proc. IEEE Int. Conf. Technol. Homeland Secur. (HST)*, Waltham, MA, USA, Apr. 2011, pp. 236–241.

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

[21] F. Björk, M. Henkel, J. Stirna, and J. Zdravkovic, "Cyber resilience–fundamentals for a definition," *Adv. Intell. Syst. Comput.*, vol. 353, pp. 3–4, Jan. 2015, doi: 10.1007/978-3-319-16486-1.

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

[23] MITRE, McLean, VA, USA. (2012). *Cyber Resiliency Metrics*. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

[24] G. Sharkov, "From cybersecurity to collaborative resiliency," in *Proc. ACM Workshop Automated Decis. Making Act. Cyber Defense, Co-Located CCS (SafeConfig)*, Vienna, Austria, 2016, pp. 3–9.

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

[26] Center for Internet Security (CIS), New York, NY, USA. (2019). *CIS Controls Version 7.1*. [Online]. Available: https://www.cisecurity.org/controls/

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

[28] World Economic Forum, Geneva, Switzerland. (2016). *A Framework for Assessing Cyber Resilience*. [Online]. Available: http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf

[29] L. F. Cranor, "A Framework for Reasoning About the Human in the Loop," in *Proc. 1st Conf. Usability, Psychol., Secur.*, San Francisco, CA, USA, 2008, pp. 1:1–1:15. [Online]. Available: http://dl.acm.org/citation.cfm?id=1387649.1387650.

[30] B. Schneier, "The future of incident response," *IEEE Secur. Privacy*, vol. 12, no. 5, pp. 96–97, Oct. 2014.

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

[32] NIST, Gaithersburg, MD, USA. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 Revision 4)*. [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

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

[34] P. A. Sharikov, "Evolution of American cyber security policies," *World Econ. Int. Relations*, vol. 63, no. 10, pp. 51–58, Oct. 2019, doi: 10.20542/0131-2227-2019-63-10-51-58.

[35] G. Cybenko, "Quantifying and measuring cyber resiliency," *Proc. SPIE*, vol. 9825, May 2016, Art. no. 98250R. [Online]. Available: http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.2230586

[36] T. Aoyama, H. Naruoka, I. Koshijima, W. Machii, and K. Seki, "Studying resilient cyber incident management from large-scale cyber security training," in *Proc. 10th Asian Control Conf. (ASCC)*, Sabah, Malaysia, May 2015, pp. 1–4.

[37] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cyber-security," *Technol. Innov. Manage.*, vol. 4, pp. 13–21, Oct. 2014, doi: 10.22215/timreview/835.

[38] J. Nys, "How to steer cyber security with only one KPI: The cyber risk resilience," in *Proc. RSA Conf.*, San Francisco, CA, USA, 2016, pp. 1–42. [Online]. Available: https://www.rsaconference.com/writable/presentations/file_upload/cxo-f02-how_to_steer_cyber_security_with_only_one_kpi_the_cyberrisk_resilience.pdf

[39] Carnegie Mellon University, Department of Homeland Security. (2016). *Cyber Resilience Review (CRR)*. Accessed: Feb. 6, 2018. [Online]. Available: https://www.us-cert.gov/ccubedvp/assessments

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

[41] E. Kädena, "Security of mobile devices in the view of Swiss cheese model," in *Kiberbiztonság/Cybersecurity*, Z. Rajnai, Ed. Budapest, Hungary: Doctoral School Secur. Sci., 2019, pp. 176–183.

[42] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "The impact of information sharing on cybersecurity underinvestment: A real options perspective," *J. Accounting Public Policy*, vol. 34, no. 5, pp. 509–519, Sep. 2015, doi: 10.1016/j.jaccpubpol.2015.05.001.

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

[44] *Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program*, ISA Standard ANSI/ISA-62443-2-1 (99.02.01), Research Triangle Park, NC, USA, 2009, pp. 1–170.

[45] ISACA, Rolling Meadows, IL, USA. (2012). *A Business Framework for the Governance and Management of Enterprise IT*. [Online]. Available: https://www.isaca.org

[46] Hong Kong Monetary Authority, Hong Kong. (2016). *Cyber Resilience Assessment Framework*. [Online]. Available: https://docplayer.net/storage/82/85773113/1595943763/PcrhUos-qhsdL04obl2tUQ/85773113.pdf
[47] *Information Technology–Security Techniques–Information Security Management Systems–Requirements*, Standard ISO/IEC 27001:2013(en), Geneva, Switzerland, 2013. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
[48] R. A. Caralli, J. H. Allen, D. W. White, L. R. Young, N. Mehravari, and P. D. Curtis. (2016). CERT resilience management model. Version 1. 2. Pittsburgh, PA, USA. [Online]. Available: https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf
[49] World Economic Forum, Geneva, Switzerland. (2017). *Advancing Cyber Resilience–Principles and Tools for Boards*. [Online]. Available: http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf
[50] Pacific Northwest National Laboratory, Washington, DC, USA. (2019). *Buildings Cybersecurity Capability Maturity Model*. Accessed: Oct. 16, 2019. [Online]. Available: https://bc2m2.pnnl.gov/
[51] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *J. Manage. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, 2007. [Online]. Available: http://www.tandfonline.com/doi/full/10.2753/MIS0742-1222240302
[52] 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. [Online]. Available: http://www.ejbrm.com/issue/download.html?idArticle=276.
[53] A. Hevner, S. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quart.*, vol. 28, no. 1, p. 75, 2004, doi: 10.2307/25148625.
[54] M. Lind, D. Rudmark, and U. Seigerroth, "Design science research for business process design: Organizational transition at intersport Sweden," in *Proc. IFIP WG Int. Working Conf.*, Perth, WA, Australia, 2010, pp. 159–176. [Online]. Available: http://link.springer.com/10.1007/978-3-642-12113-5_10
[55] 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.
[56] 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.
[57] 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, May 2018, doi: 10.1080/23738871.2018.1520271.
[58] B. G. Glaser and A. L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Piscataway, NJ, USA: Transaction Publishers, 2009.
[59] G. A. Bowen, "Document analysis as a qualitative research method," *Qualitative Res. J.*, vol. 9, no. 2, pp. 27–40, Aug. 2009, doi: 10.3316/QRJ0902027.
[60] J. Corbin and A. L. Strauss, *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*, 4th ed. Thousand Oaks, CA, USA: Sage Publications, 2014.
[61] J. Saldaña, *The Coding Manual for Qualitative Researchers*, 3rd ed. Thousand Oaks, CA, USA: SAGE Publications, 2015.
[62] B. G. Glaser, *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*, 5th ed. Mill Valley, CA, USA: Sociology Press, 1978.
[63] M. Wiesche, M. C. Jurisch, P. W. Yetton, and H. Krcmar, "Grounded theory methodology in information systems research," *MIS Quart.*, vol. 41, no. 3, pp. 685–701, Mar. 2017, doi: 10.25300/MISQ/2017/41.3.02.
[64] A. L. Strauss, *Qualitative Analysis for Social Scientists*. Cambridge, U.K.: Cambridge Univ. Press, 1987.
[65] N. Kshetri, *The Global Cybercrime Industry*, 1st ed. Berlin, Germany: Springer, 2010.
[66] Ponemon Institute. Traverse City, MI, USA. (2012). *2011 Cost of Data Breach Study: Australia*. [Online]. Available: https://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-australia-us.pdf
[67] J. F. Carías, L. Labaka, J. M. Sarriegi, and J. Hernantes, "Defining a cyber resilience investment strategy in an industrial Internet of Things context," *Sensors*, vol. 19, no. 1, p. 138, Jan. 2019, doi: 10.3390/s19010138.
[68] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Comput. Hum. Behav.*, vol. 48, pp. 51–61, Jul. 2015, doi: 10.1016/j.chb.2015.01.039.
[69] F. B. Saghezchi, G. Mantas, J. Ribeiro, A. Esfahani, H. Alizadeh, J. Bastos, and J. Rodriguez, "Machine learning to automate network segregation for enhanced security in industry 4.0," in *Proc. Int. Conf. Broadband Commun., Netw. Syst.*, 2019, pp. 149–158. [Online]. Available: http://link.springer.com/10.1007/978-3-030-05195-2_15
[70] N. Wirth, "Program development by stepwise refinement," *Commun. ACM*, vol. 26, no. 1, pp. 70–74, Jan. 1983, doi: 10.1145/357980.358010.
[71] C. Tupper, *Data Architecture: From Zen to Reality*, 1st ed. Amsterdam, The Netherlands: Elsevier, 2011.
[72] M. Sokovich, D. Pavletic, and K. K. Pipan, "Quality improvement methodologies–PDCA cycle, RADAR matrix, DMAIC and DFSS," *J. Achievements Mater. Manuf. Eng.*, vol. 43, no. 1, pp. 476–483, Oct. 2010. [Online]. Available: https://www.semanticscholar.org/paper/Quality-improvement-methodologies%3A-PDCA-cycle%2C-and-Pipan/e3488a24ab1197670544b4e08dc6173f396eada9
[73] A. M. Davis, E. H. Bersoff, and E. R. Comer, "Software system engineering process models," in *Software Requirements Engineering*, vol. 14, 2nd ed. Hoboken, NJ, USA: Wiley, Oct. 2011, pp. 456–463.
[74] Gupta and Zhdanov, "Growth and sustainability of managed security services networks: An economic perspective," *MIS Quart.*, vol. 36, no. 4, p. 1109, 2012, doi: 10.2307/41703500.
[75] C. W. Liu, P. Huang, and H. C. Lucas, "IT centralization, security outsourcing, and cybersecurity breaches: Evidence from the U.S. Higher education," in *Proc. Transforming Soc. Digit. Innov. (ICIS)*, 2017, p. 18. [Online]. Available: http://penghuang.com/WordPress/wp-content/uploads/2018/12/IT-Centralization-Security-Outsourcing-and-Cybersecurity-Breach.pdf
[76] J. J. Wang and D. L. Yang, "Using a hybrid multi-criteria decision aid method for information systems outsourcing," *Comput. Oper. Res.*, vol. 34, no. 12, pp. 3691–3700, 2007, doi: 10.1016/j.cor.2006.01.017.
[77] V. Grover, M. J. Cheon, and J. T. C. Teng, "A descriptive study on the outsourcing of information systems functions," *Inf. Manag.*, vol. 27, no. 1, pp. 33–44, 1994, doi: 10.1016/0378-7206(94)90100-7.
[78] K. Ketler and J. Walstrom, "The outsourcing decision," *Int. J. Inf. Manage.*, vol. 13, no. 6, pp. 449–459, 1993, doi: 10.1016/0268-4012(93)90061-8.
[79] C. Yang and J.-B. Huang, "A decision model for IS outsourcing," *Int. J. Inf. Manage.*, vol. 20, no. 3, pp. 225–239, Jun. 2000, doi: 10.1016/S0268-4012(00)00007-4.

JUAN FRANCISCO CARÍAS received the B.S. degree in industrial management engineering from the TECNUN, School of Engineering, University of Navarra, Donostia-San Sebastian, Spain, in 2017. He is currently pursuing the Ph.D. degree in applied engineering with the TECNUN, University of Navarra.

From 2017 to 2019, he has been a Researcher with the Department of Industrial Management Engineering, TECNUN. His research interests include the management of cyber resilience, cyber resilience building methodologies, and cyber resilience awareness-raising tools. He was a recipient of the Kutxa Fundazioa Award for Best Academic Record in industrial management engineering in 2017.

MARCOS R. S. BORGES (Member, IEEE) received the M.S. degree in systems and computing engineering from the Federal University of Rio de Janeiro, Brazil, in 1981, and the Ph.D. degree in computer science from the University of East Anglia, U.K., in 1986.

From 1994 to 1996, he was a Visiting Research Scholar with the Object Technology Laboratory, Santa Clara University, Santa Clara, CA, USA. He has served as a Visiting Professor at the University of Paris VI, in 2001, and at the Polytechnic University of Valencia, Spain, from 2004 to 2005. He is currently a Full Professor of computer science with the Federal University of Rio de Janeiro, Brazil. He is also a Visiting Professor with the TECNUN, University of Navarra. He has published over 100 research articles in international conferences and journals, including *Decision Support Systems*, *Computers in Industry*, *Information Sciences*, and *Expert Systems with Applications*. His research interests include CSCW, group decision support systems, resilience engineering, and collective knowledge. He is also a member of the ACM and the ISCRAM Association. He is a member of the Systems, Man and Cybernetics Society and a Steering Committee Member of the CSCWD Technical Committee. He was a former President of ISCRAM Association.

LEIRE LABAKA received the B.S. and M.S. degrees in industrial engineering and the Ph.D. degree in applied industrial engineering from the University of Navarra, Spain, in 2009 and 2013, respectively. Since 2013, she has been a Professor of modelling and simulation, business administration and accounting and finance with the University of Navarra. She has published in several articles in indexed journals, 26 indexed in JCR, whereby 10 of them in the first quartile (Q1), and 47 indexed in SCOPUS. Furthermore, she has also published 12 book chapters and several proceedings in highly relevant international conferences. Her research interests include resilience, climate change, urban sustainability, critical infrastructure protection, and cyber resilience. She has taken part in SMR, ELITE, and SEMPOC projects funded by the European Commission in the H2020, FP7, and CIPS research programs as well as in four industrial projects.

SAIOA ARRIZABALAGA received the M.Sc. degree in telecommunication engineering from the Faculty of Engineering in Bilbao (University of the Basque Country), Spain, in 2003, and the Ph.D. in Engineering degree from the TECNUN, University of Navarra, Spain, in 2009.

She joined the CEIT Research Centre, Donostia-San Sebastian, in 2003, as a Research Assistant. She also worked as a Teaching Collaborator with the TECNUN, University of Navarra, Donostia-San Sebastian, from 2005 to 2009, where she has been a Lecturer since 2009. She is currently the Head of the Data Analysis and Information Management Research Group and the Co-Director of the Information and Communication Technologies' Division, CEIT. She has been involved in 22 international or national research projects (being the coordinator of 12 of them), has co-directed five doctoral theses and has contributed in more than 50 international and national journal and conferences. Her current interests include data analytics and cybersecurity topics.

JOSUNE HERNANTES received the M.S. degree in computer science from Basque Country University, Spain, in 2002, and the Ph.D. in Engineering degree from the University of Navarra, Spain, in 2008. Since 2009, she has been a Professor of computer science and software engineering with the University of Navarra. She has published in several articles in indexed journals, 35 indexed in JCR, whereby 10 of them in the first quartile (Q1), and 54 indexed in SCOPUS. Furthermore, she has also published several book chapters and several articles in proceedings in highly relevant international conferences. She has taken part in SMR, ELITE, and SEMPOC projects funded by the European Commission in the H2020, FP7, and CIPS research programs. She has also been involved in 12 national research projects. Her research interests include resilience, climate change, urban sustainability, critical infrastructure protection, and cyber resilience.