Politehnica University Timișoara
Doctoral School of Engineering
PhD in the Field of ENGINEERING AND MANAGEMENT

SUMMARY
OF PhD THESIS

CONTRIBUTIONS TO CYBERSECURITY RISK MANAGEMENT: IoT SECURITY RISK MANAGEMENT STRATEGY REFERENCE MODEL (IoTSRM2)

PhD Candidate: **Traian Mihai POPESCU**

PhD Supervisor: **Prof. Gabriela PROȘTEAN, PhD**

TIMIȘOARA 2021

Table of Contents

Table of Contents of the PhD Thesis

Chapter 1. Introduction

Chapter 1 provides the background of, motivation for, objectives of, and the structure of this thesis. First, **Chapter 1.1** is structured in the background of cybersecurity risk management and the background of Internet of Things (IoT). Hence, with respect to the background of cybersecurity risk management, the subchapter outlines some of the possible implications for organizations operating in the current digital transformation era from the perspective of cybersecurity, introduces some of the key cybersecurity risk management concepts, and provides overviews of several renowned cybersecurity risk management standards and methodologies. In terms of the possible implications for organizations embracing technological advances, these include the widening of the attack surface, the incessant evolution of the cyber threat landscape, the ever-growing cybersecurity regulatory ecosystem, and in turn the need to continuously improve the cybersecurity risk management practices in organizations. Furthermore, the subchapter defines and outlines some of the main cybersecurity risk management concepts relevant for this thesis, namely some key cybersecurity-related terms, the cybersecurity risk management process, and six cybersecurity domains relevant for cybersecurity risk management strategy. Moreover, the subchapter provides an overview of the cybersecurity risk management standards which focuses on two categories of standards (i.e., cybersecurity risk management, and generic risk management) that can be leveraged by any organization regardless of type, size, or sector. Hence, with respect to the cybersecurity risk management standards, eight standards were outlined that provide requirements for ISMS, general guidelines for ISMS, general guidelines for information security risk management, guidelines on cybersecurity, or requirements for cybersecurity risk management. About the generic risk management standards, three standards were outlined that provide principles and guidelines on risk management or guidelines on risk assessment. Furthermore, Figure 1.1 outlines the selected standards relevant to each of the two categories of standards.

Figure 1.1. Selected standards related to cybersecurity risk management

Furthermore, the subchapter provides an overview of the cybersecurity risk management methodologies which includes a few notable methodologies that match one of the following three categories: cybersecurity risk assessment, cybersecurity risk management, and cybersecurity maturity assessment. Hence, four methodologies were outlined for the cybersecurity risk assessment category, one methodology was described for the cybersecurity risk management category, and one methodology was outlined for the cybersecurity maturity assessment category. Furthermore, Figure 1.2 highlights the methodologies selected for each of the three categories of methodologies.

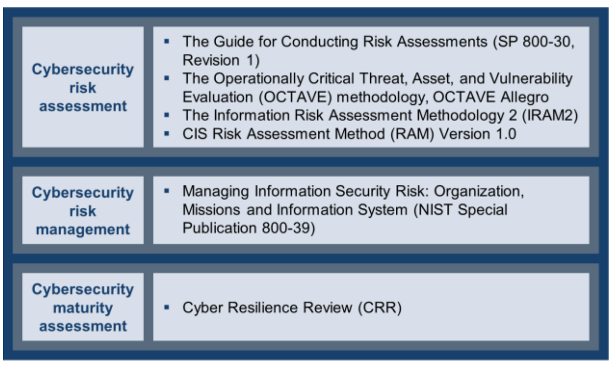

Figure 1.2. Selected cybersecurity risk management methodologies

Then, with respect the background of Internet of Things (IoT), the subchapter outlines the various application areas of the IoT (e.g., healthcare, environmental, commercial, industrial, smart cities, and infrastructural applications), different projections for IoT adoptions highlighting the common consensus for IoT growth, and it introduces some of the key IoT concepts including the components of the ITU-T's reference model for IoT [ITU12].

Afterwards, **Chapter 1.2** provides the motivation for this research work by making reference to the top three challenges faced by organizations (i.e., the rising cybersecurity risks, difficulty in adopting new technologies, and poor risk management practices) [ATK18]. The subchapter indicates that these challenges are linked to the prevalence of reactive cybersecurity strategies [Nat17], to the difficulty in securely adopting IoT, and to the widespread absence of robust IoT security risk management strategies in organizations. In this context, Figure 1.3 examplifies how cybersecurity, cybersecurity risk management, IoT security, and IoT security risk management topics fit together, and highlights the topics of interest of this thesis (i.e., cybersecurity risk management and IoT security risk management).

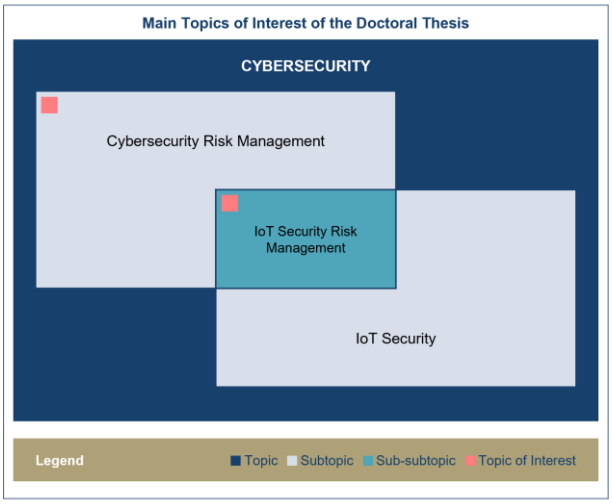

Fig. 1.3. Topics of interest of the doctoral thesis

Then, the subchapter provides the rationale behind focusing on key drivers of and enablers for cybersecurity risk management by pointing out the linkage between the key drivers and the importance of strategic analysis for effective strategy formulation, and the linkage between the key enablers and the importance of making use of planning instruments for achieving actionable strategies. Subsequently, the subchapter provides the rationale behind focusing this doctoral thesis on the four focus areas (i.e., cyber threat landscape, cybersecurity regulatory landscape, cybersecurity risk management frameworks, and IoT security best pactices) along with the corresponding thesis objectives.

Then, **Chapter 1.3** provides the objectives of my thesis, which are enumerated below:

- **Objective 1:** Provide an overview of the current cybersecurity threats of organizations;
- **Objective 2:** Provide an overview of the cybersecurity regulatory landscape focused on key cybersecurity-related legislations and regulations from key cybersecurity jurisdictions;
- **Objective 3:** Provide an overview of several well-renowned cybersecurity risk management frameworks;
- **Objective 4:** Provide an overview of the IoT security best practices and classify these best practices using a proposed taxonomic hierarchy;
- **Objective 5:** Propose a cyber threat rating method that aims to reduce the complexity and uncertainty attached to the existing threat rating methods and prioritize current cyber threats using this proposed method;
- **Objective 6:** Propose a method for evaluating key cybersecurity-related legislations to establish the degree of commonality between them from the perspective of the organizational understanding to managing cybersecurity risk and provide a critical evaluation of in-scope cybersecurity-related legislations based on the proposed method;
- **Objective 7:** Propose a methodology for evaluating cybersecurity risk management frameworks and provide a critical evaluation of in-scope cybersecurity risk management frameworks based on the proposed methodology;
- **Objective 8:** Propose a methodology for developing a reference model for IoT security risk management strategy, propose the IoT security risk management strategy reference model

(IoTSRM2), and evaluate the proposed IoTSRM2 against the IoT security best practices that are the most relevant for the proposed model;

- **Objective 9:** Propose a methodology for undertaking a survey study to determine the current state of IoT security risk management strategies in the surveyed organizations relative to the proposed IoTSRM2, conduct the survey study based on the proposed methodology, and report the survey findings based on the proposed methodology.

Finally, **Chapter 1.4** provides the outline of my thesis as depicted in Figure 1.4, which also maps the thesis objectives to the thesis chapters and/or subchapters where they are achieved, and provides a reading map for the thesis objectives. With respect to the reading map, this mapping should be leveraged in conjunction with the nine objectives of this thesis by readers interested in specific thesis objectives, where:

- **Mapping 1** corresponds to the outputs of my research work on the cyber threat landscape, which concretized in the achievement of the Objective 1 and Objective 5;
- **Mapping 2** corresponds to the outputs of my research work on the cybersecurity regulatory landscape, which concretized in the achievement of the Objective 2 and Objective 6;
- **Mapping 3** corresponds to the outputs of my research work on the cybersecurity risk management frameworks, which concretized in the achievement of the Objective 3 and Objective 7;
- **Mapping 4** corresponds to the outputs of my research work on the IoT security best practices, which concretized in the achievement of the Objective 4, Objective 8, and Objective 9.

For instance, assuming a reader is interested in Objective 9, Figure 1.4 guides the reader via "Mapping 4" to read Chapters 1, 2.4, 5, 6, and 7.

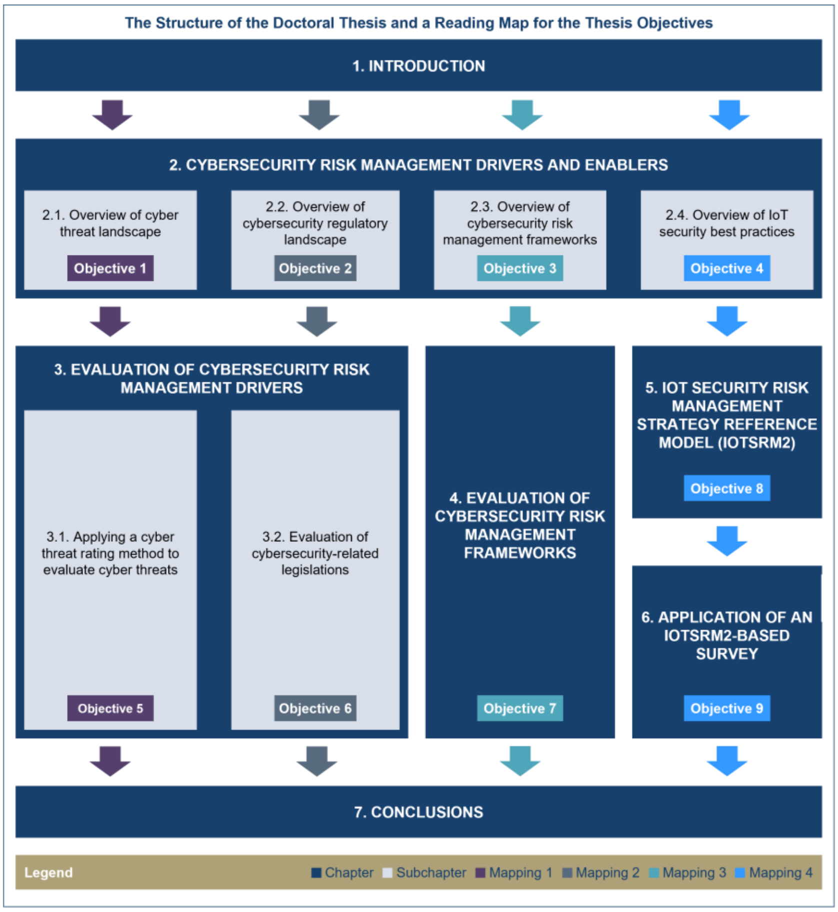

Figure 1.4. The thesis structure and a reading map for the thesis objectives

Chapter 2. Cybersecurity Risk Management Drivers and Enablers

Chapter 2 presents overviews of the key drivers of and enablers for cybersecurity risk management in organizations. About the key cybersecurity risk management drivers, the chapter focuses on outlining the current state of the cyber threat and cybersecurity regulatory landscapes, and about the key cybersecurity risk management enablers, the chapter focuses on outlining the current state of cybersecurity risk management frameworks and IoT security best practices.

Hence, **Chapter 2.1** provides an overview of the cyber threat landscape with the purpose of reducing the complexity attached to carrying out cybersecurity risk assessments within organizations and to enable them to keep pace with the ever-evolving cyber threat landscape. This overview was achieved by consolidating and categorizing the most frequently encountered cyber threats from seventeen relevant and well-renowned sources, including nine threat landscape reports, two survey reports on cybersecurity incidents and data breaches, one European law enforcement report on cybercrime, one survey report on the global state of cybersecurity, one insight report on cybersecurity considerations, two insight reports on cybersecurity incident investigations, and one report on cybersecurity trends. Thus, based on the investigation of these seventeen sources, thirteen up-to-date cyber threat categories were determined and described, namely the malware attacks, social engineering attacks, denial of service (DoS), spam, insider threat, hacking attacks, attacks on privacy and personal data, cryptojacking, cyber espionage, targeted attacks on critical infrastructure, supply chain attacks, cyberpropaganda, and legal and regulatory sanctions.

Furthermore, the study of the literature on the cyber threat landscape revealed the need for a cyber threat rating method that is dissociated from the elements (e.g., skill level, motive, opportunity) that induce uncertainty, and this aspect motivated the proposed cyber threat rating method from **Chapter 3**.

Then, **Chapter 2.2** provides an overview of the cybersecurity regulatory landscape by targeting key cybersecurity-related legislations and regulations from key cybersecurity jurisdictions, and it aims to set the scene for establishing the degree of commonality between these legislations from the perspective of the organizational understanding to managing cybersecurity risk. Hence, this overview of cybersecurity-related legislations and regulations exclusively focused on the jurisdictions (i.e., European Union, Singapore, United States) that exhibited the highest levels of commitment towards cybersecurity across the globe based on the Global Cybersecurity Index (GCI) report [ITU17], it concentrated on the most relevant cybersecurity-related areas of statute (i.e., the data protection and privacy area and critical infrastructure protection area) for triggering the improvement of cybersecurity risk management practices in organizations, and it centred on the statutes that were generally applicable and in force at the time of conducting the study [Giu+21]. Moreover, this overview of cybersecurity-related legislations and regulations excluded statutes related to specific cybersecurity products or services, sector specific cybersecurity legislations and regulations, laws and regulations which were not enacted at the time of conducting the study, legislations and regulations pertaining to other cybersecurity-related areas of statute (e.g., export control, cybercrime), laws applicable to specific EU Member States or US's Member States, and international cooperation agreements on cybersecurity.

Hence, with respect to the European Union, the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Directive on Security of Network and Information Systems (NISD) were identified for the data protection and privacy area and for the critical infrastructure protection area, respectively. About Singapore, the Personal Data Protection Act 2012 (PDPA) and the Cybersecurity Act (CA) were identified for the data protection and privacy area and for the critical infrastructure protection area, respectively. As for the United States, there was no generally applicable data protection- and privacy-related legislation found at federal level, and the Critical Infrastructures Protection Act of 2001, the Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, the Presidential Policy Directive on Critical Infrastructure Security and Resilience, and the Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure were identified for the critical infrastructure protection area. It is worth noting that the NIST's Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF) [NIS18a] was identified as being the by-product of the US legislation pertaining to the critical infrastructure protection area.

Furthermore, this overview revealed the need for critical evaluations of selected cybersecurity-related legislations to establish the degree of commonality between them, and this aspect motivated the critical evaluation of cybersecurity-related legislations from **Chapter 3**.

Afterwards, **Chapter 2.3** provides an overview of several well-renowned cybersecurity risk management frameworks by defining the "cybersecurity risk management framework" and by outlining some of the most widely adopted frameworks for managing cybersecurity risks. In this context, these frameworks were selected to be leveraged by any organization regardless of type, size, sector, or focus area, and grouped into three categories relevant for cybersecurity risk management (i.e., cybersecurity-related frameworks, generic risk management frameworks, and IT-related frameworks). With respect to the cybersecurity-related frameworks, ten frameworks were outlined that are applicable to either risk assessment or risk management activities and are supported by a risk-based or compliance-based approach. About the generic risk management frameworks, three frameworks were outlined that provide generic control objectives, internal controls, principles, or guidelines on risk management. As for the IT-related frameworks, four frameworks were outlined that belong to the following focus areas: IT service management, enterprise IT governance and management, enterprise-wide IT risk management, or IT capability management. Furthermore, Figure 2.1 outlines the selected frameworks pertaining to these three categories relevant to cybersecurity risk management.

Figure 2.1. Selected cybersecurity risk management frameworks

Furthermore, the overview revealed the need for critical evaluations of cybersecurity risk management frameworks relative to each other to support decision making when it comes to framework selection, and this aspect motivated the critical evaluation of the cybersecurity risk management frameworks from **Chapter 4**.

Then, **Chapter 2.4** proposes a novel taxonomic hierarchy for classifying IoT security best practices based on their target audience group (i.e., adopter specific, general, manufacturer specific, and supplier specific) and type (i.e., codes of practice, standards, guidelines, and frameworks), and then it provides a comprehensive overview of 25 selected IoT security best practices which were classified using the proposed taxonomic hierarchy. Furthermore, Figure 2.4 shows the proposed taxonomic hierarchy for classifying IoT security best practices.

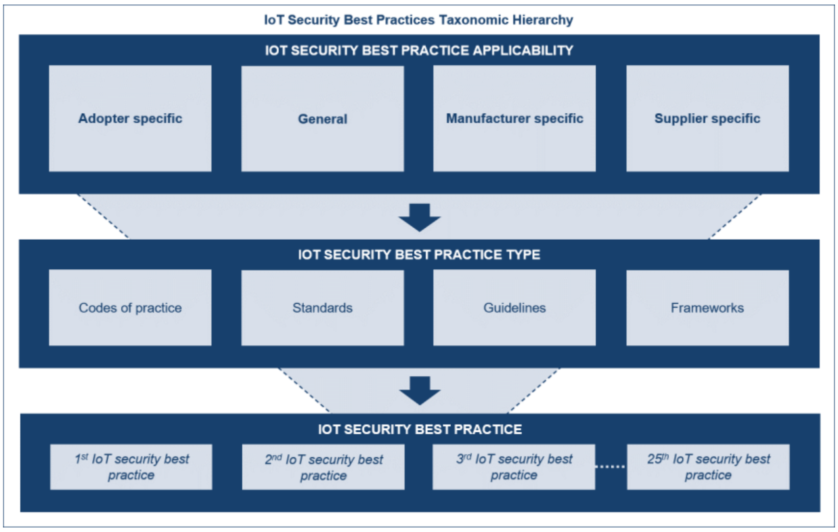

Figure 2.2. The proposed taxonomic hierarchy for IoT security best practices [Pop+21a]

The identification of the in-scope IoT security best practices was based on the study of the literature on IoT security best practices, and it disregarded the exclusively technically-focused IoT security best practices, IoT security best practices intended for the purpose of certification, draft or expired versions of IoT security best practices, cybersecurity best practices that are not IoT security specific, and vendor reports that address IoT security best practices.

Hence, about the adopter specific IoT security best practices, this subchapter outlined one IoT security framework and three guidelines where each of these guidelines focuses on generic-based IoT security controls, IoT recommendations specific to Identity and Access Management, or healthcare-specific IoT security good practices. Furthermore, Figure 2.5 shows the selected adopter specific IoT security best practices.

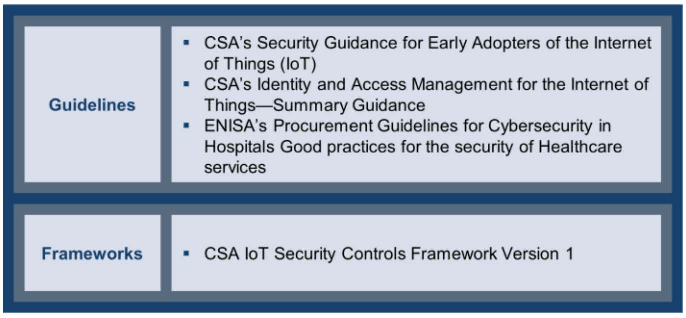

Figure 2.3. The selected adopter specific IoT security best practices. Adapted from [Pop+21a]

With respect to the general IoT security best practices, the subchapter outlined two codes of practice that focus on secure IoT systems development lifecycle, two guidelines that target sector-specific organizations, one guideline for IoT systems development lifecycle, one guideline for secure IoT supply chain, and three frameworks that address strategic principles or trustworthiness requirements. Furthermore, Figure 2.6 shows the selected general IoT security best practices.

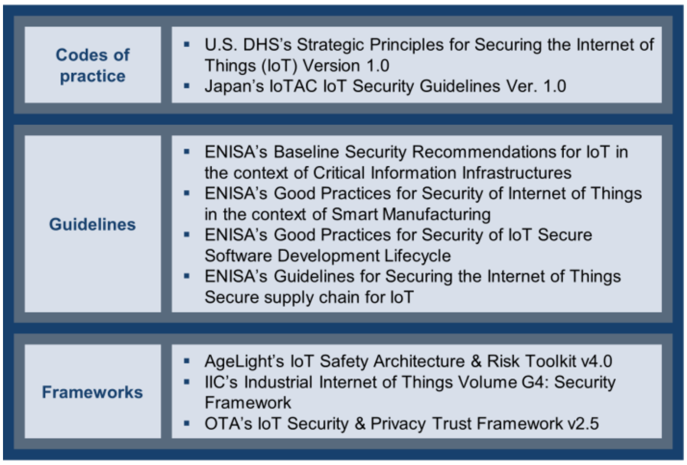

Figure 2.4. The selected general IoT security best practices. Adapted from [Pop+21a]

Regarding the manufacturer specific IoT security best practices, this subchapter outlined two IoT security standards and four guidelines that give security recommendations, baseline capabilities, or principles for IoT devices. Furthermore, Figure 2.7 shows the selected manufacturer specific IoT security best practices.

Figure 2.5. The selected manufacturer specific IoT security best practices. Adapted from [Pop+21a]

As for the supplier specific IoT security best practices, the chapter outlined two codes of practice that provide IoT security measures, two IoT security guidelines, and two IoT security frameworks. Furthermore, Figure 2.8 shows the selected supplier specific IoT security best practices.

Figure 2.6. The selected supplier specific IoT security best practices. Adapted from [Pop+21a]

In addition, the study revealed the need for an IoT security risk management strategy reference model, and this aspect motivated the development of the proposed reference model for IoT security risk management strategy from **Chapter 5**.

Chapter 3. Evaluation of Cybersecurity Risk Management Drivers

Chapter 3 extends the research work on the cybersecurity risk management drivers (i.e., the cyber threat landscape and the cybersecurity regulatory landscape) outlined in **Chapter 2**. Hence, with respect to the research work on the cyber threat landscape, this chapter aims to support the prioritization of the cyber threats based on their potential to inflict cyber harm on organizations and their stakeholders and to enable the formation of a more holistic depiction of some of the most current cyber threats by addressing the need for a cyber threat rating method based on measurable elements [Pop+19b]. As for the research work on the cybersecurity regulatory landscape, this chapter aims to alleviate the degree of complexity associated with achieving organizational compliance with cybersecurity-related legislations and regulations by addressing the need for critical evaluations of selected cybersecurity-related legislations to establish the degree of commonality between them [Pop+19a].

In this context, **Chapter 3.1** provides a novel cyber threat rating method which allows the analysis of the in-scope cyber threat categories, the estimation of the extents of their applicability to cyber harm based on the latest taxonomy of organizational cyber harm developed by Agrafiotis et al. (2018) [Agr+18], and the prioritization of the in-scope cyber threat categories. The taxonomy of cyber harm consists of the "Physical/Digital", "Economic", "Psychological", "Reputational", and "Social/Societal" types of cyber harms with fifteen, sixteen, twelve, ten, and four sub-types of cyber harm, respectively. Furthermore, this taxonomy is represented using six equations, where one equation represents the types of cyber harm, and the remaining five equations represent the sub-types of each type of cyber harm. For instance, the Equation (3.1) is used to represent the sub-types (i.e., y_{1j}) of the "Physical/Digital" type of cyber harm (i.e., y_1):

$$y_{1j} = \left\{ \begin{array}{c} \text{Damaged or unavailable, Destroyed, Theft,} \\ \text{Compromised, Infected, Exposed / leaked,} \\ \text{Corrupted, Reduced performance,} \\ \text{Bodily injury, Pain, Loss of life,} \\ \text{Prosecution, Abuse, Mistreatment,} \\ \text{Identity theft} \end{array} \right\}, \text{ where } j = [1..15] \tag{3.1}$$

Moreover, this cyber threat rating method introduced several equations that allow the calculus associated with the determination of the extent to which a certain cyber threat category is potentially applicable to a specific and across all types of cyber harm. Hence, the proposed cyber threat rating method involves rating each cyber threat category of the set of in-scope cyber threat categories (i.e., x_k) against all sub-types (i.e., y_{ij}) of each type of cyber harm (i.e., y_i) using the Equation (3.2), where $\text{Rating}_{x_k}\left(y_{ij}\right)$ is this rating, C is the cardinality of the set of in-scope cyber threat categories (i.e., x_k), and n_i is the number of sub-types corresponding to each type of cyber harm:

$$\text{Rating}_{x_k}\left(y_{ij}\right) = \begin{cases} 1, \text{ if the sub-type is applicable for } x_k \\ 0, \text{ otherwise} \end{cases}, \\ \text{where } k=[1..C],\ C=|x_k|,\ i = [1..5],\ j = [1..n_i] \tag{3.2}$$

Subsequently, for each cyber threat category of the set of in-scope cyber threat categories, the ratings corresponding to the sub-types of each type of cyber harm are summed to score the extent to which the cyber threat category in question is potentially applicable to a specific type of cyber harm using the Equation (3.3):

$$\text{Threat rating } (x_k) = \sum_{j=1}^{n_i} \text{Rating}_{x_k}\left(y_{ij}\right), \text{ where } k=[1..C],\ C=|x_k|,\ i = [1..5] \tag{3.3}$$

Then, the resulting scores are weighted by $1/n_i$, where n_i is the number of sub-types pertaining to each type of cyber harm. These weighted scores enable the comparisons between the possible extents to which a specific cyber threat category of the set of in-scope cyber threat categories applies to different types of cyber harm, and between the in-scope cyber threat categories in relation to the possible extents to which they apply to a specific type of cyber harm. Finally, for each cyber threat category of the set of in-scope cyber threat categories, the resulting scores for the types of cyber harm are summed to indicate the extent to which that in-scope cyber threat category applies across all five types of cyber harm. For each cyber threat category of the set of in-scope cyber threat categories, the resulting scores are weighted by 1/5, where 5 is the number of types of cyber harm. These overall scores provide a mean to compare the in-scope cyber threat categories based on the possible extents of applicability to cyber harm considering the selected taxonomy of cyber harm. In addition, all weighted scores are expressed as percentages and are translated into qualitative ratings on a five-point scale (i.e., "Very Low": 0-20%, "Low": 21-40%, "Medium": 41-60%, "High": 61-80%, "Very High": 81-100%).

Afterwards, this cyber threat rating method was applied to the thirteen cyber threat categories from **Chapter 2** using an Excel-based threat rating tool which was created to facilitate the determination of the threat ratings and the subsequent evaluation of the in-scope cyber threat categories.

Furthermore, the chapter provides a critical evaluation of the thirteen cyber threat categories based on their threat ratings that resulted from applying the cyber threat rating method, which allowed the prioritization of these cyber threat categories. Thus, Figure 3.1 provides the outputs of the threat rating tool for each in-scope cyber threat category in relation to the types of cyber harm.

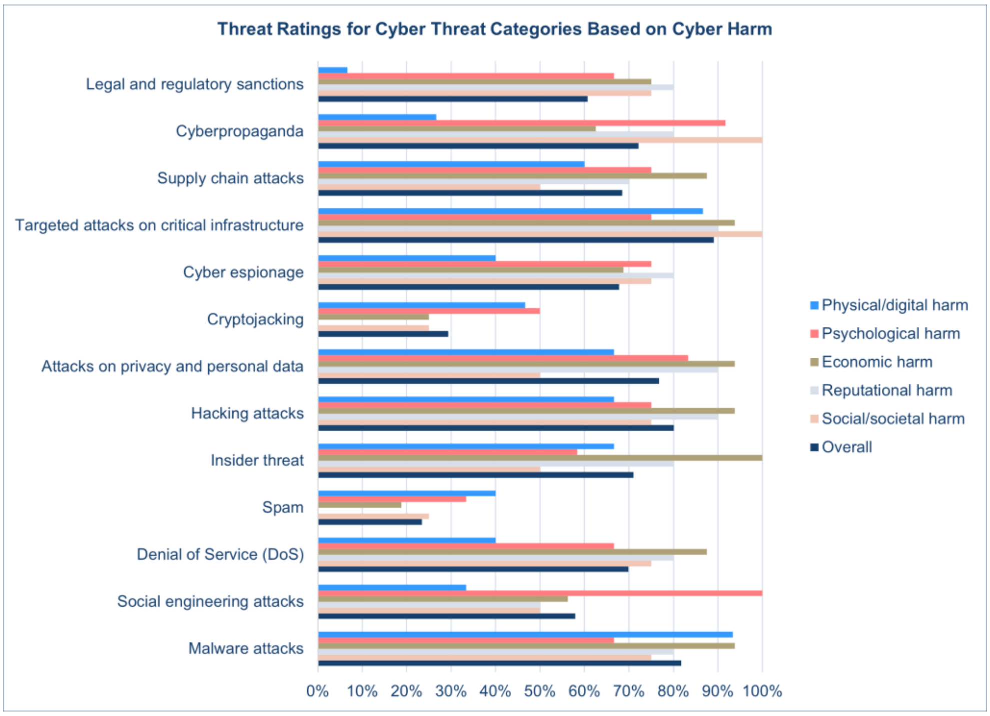

Figure 3.1. Threat ratings for in-scope cyber threat categories based on cyber harm [Pop+19b]

This evaluation revealed that three, seven, one, and two cyber threat categories exhibit "Very High", "High", "Medium", and "Low" extents of applicability to cyber harm, respectively. About the "Very High" extent of applicability to cyber harm, the "Targeted attacks on critical infrastructure", "Malware attacks", and "Hacking attacks" threat categories resulted in having scores that match the "Very High" rating. Thus, these cyber threat categories should be at the top of the list when it comes to cyber threats. With respect to the "High" extent of applicability to cyber harm, the "Attacks on privacy and personal data", "Cyberpropaganda", "Insider threat", "Denial of Service (DoS)", "Supply chain attacks", "Cyber espionage", and "Legal and regulatory sanctions" threat categories resulted in having scores that match the "High" rating. Thus, although these cyber threat categories are not at the top of the list when it comes to cyber threats, they should be of focal interest for organizations aiming to address cyber threats. Regarding the "Medium" extent of applicability to cyber harm, the "Social engineering attacks" threat category resulted in having a score that matches the "Medium" rating. Hence, although this cyber threat category appears less threatening than the ones displaying higher extents of applicability to cyber harm, it should still be seriously addressed by organizations considering that it may be an attack vector for other cyber threats. As for the "Low" extent of applicability to cyber harm, the "Cryptojacking" and "Spam" threat categories resulted in having scores that match the "Low" rating. Hence, although these cyber threat categories are the top least applicable to cyber harm among the thirteen cyber threat categories, they should not be overlooked by organizations when it comes to cyber threats as these two threat categories are not negligible.

Furthermore, Figure 3.2 shows another consolidated view of the overall ratings for the thirteen cyber threat categories.

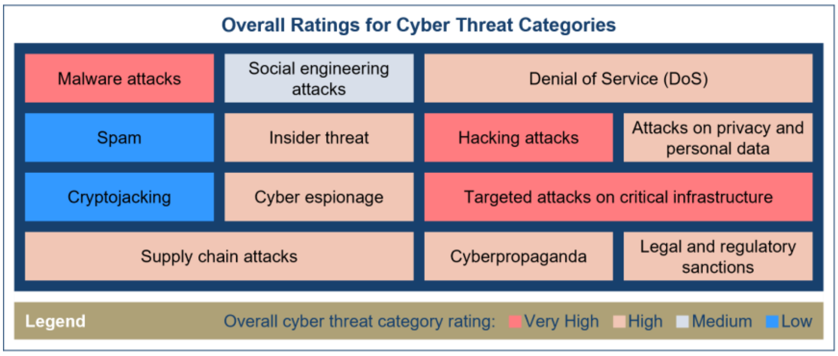

Figure 3.2. Overall ratings for the thirteen cyber threat categories based on potential cyber harm

Then, the chapter provides the findings derived from the review of the related work. Hence, one of the main findings was that the proposed cyber threat rating method leverages the latest taxonomy of cyber harm in new ways that were not previously explored.

Afterwards, **Chapter 3.2** presents a proposed method for evaluating selected cybersecurity-related legislations from the perspective of organizational understanding of cybersecurity risk management, which is based on the overview of the key cybersecurity-related legislations of the key cybersecurity jurisdictions from **Chapter 2.2** and on the NIST CSF Identify Function. Hence, this evaluation method focused on the cybersecurity-related areas of legislation (i.e., the data protection and privacy and the critical infrastructure protection areas) that trigger improvement of cybersecurity risk management practices in organizations and on the jurisdictions that demonstrated the highest levels of cybersecurity commitment worldwide (i.e., the EU, Singapore, and US).

First, the proposed evaluation method gave the rationale for basing the critical evaluation on the NIST CSF Identify Function [NIS18a]. Second, the proposed evaluation method introduced the underlying categories of the NIST CSF Identify Function (i.e., "Asset Management", "Business Environment", "Governance", "Risk Assessment", "Risk Management Strategy", "Supply Chain Risk Management"), which were used for comparing the in-scope legislations. Third, the cybersecurity-related laws and regulations from **Chapter 2.2** and the absence of a generally applicable data protection and privacy law in the US at federal level were reiterated. Subsequently, the proposed evaluation method provided the rationale for exclusively focusing on the NIST CSF rather than specific US legislation on the critical infrastructure protection area, namely for the purposes of reducing redundancy given the NIST CSF is the by-product of the US law on critical infrastructure protection. Then, the proposed evaluation method provided the in-scope cybersecurity-related legislations (i.e., the General Data Protection Regulation - GDPR, Personal Data Protection Act 2012 - PDPA, Directive on Security of Network and Information Systems - NISD, Cybersecurity Act - CA) for the critical evaluation. Moreover, the proposed evaluation method provided the definitions of the linguistic value ratings (i.e., "True", "Fairly True", "Partly True", "Nearly False", "False") used for representing the outcomes of the evaluation. First, the "True" value was used to indicate that the statute comprises requirements that fully correspond to the NIST CSF category with no apparent discrepancies. Second, the "Fairly True" value was used to indicate that the statute comprises requirements that fairly correspond to the NIST CSF category with minor discrepancies. Third, the "Partly True" value was used to indicate that the statute comprises requirements that partly correspond to the NIST CSF category with some discrepancies. Fourth, the "Nearly False" value was used to indicate that the statute comprises requirements that nearly deviate from the NIST CSF category with some similarities. Finally, the "False" value was used to indicate that the statute comprises requirements that deviate from the NIST CSF category with major discrepancies.

Then, the chapter provides the critical evaluation of the in-scope cybersecurity-related legislations to identify their degree of commonality and support a pragmatic approach to attaining regulatory compliance for organizations striving to prevent the sanctions and costly lawsuits following law infringements. Thus, Table 3.1 summarizes the findings of the evaluation for each selected cybersecurity-related legislation in relation to the categories of the NIST CSF Identify Function.

Table 3.1. Results of the evaluation of the in-scope legislations [Pop+19a]

Unique ID.	NIST CSF Category	GDPR	PDPA	NISD	CA
ID.AM	Asset Management	Fairly True	Nearly False	True	True
ID.BE	Business Environment	Partly True	Nearly False	Fairly True	Partly True
ID.GV	Governance	Fairly True	Partly True	True	Partly True
ID.RA	Risk Assessment	Partly True	Nearly False	Fairly True	Fairly True
ID.RM	Risk Management Strategy	Partly True	Nearly False	Fairly True	Nearly False
ID.SC	Supply Chain Risk Management	Fairly True	Nearly False	Fairly True	Nearly False

Hence, with respect to the "Asset Management" category of the NIST CSF Identify Function, the requirements of CA and NISD fully correspond to this category with no apparent discrepancies and the GPDR's requirements fairly correspond to this category with minor discrepancies. About the "Business Environment" category of the NIST CSF Identify Function, the NISD's requirements fairly correspond to this category with minor discrepancies. Regarding the "Governance" category of the NIST CSF Identify Function, the NISD's requirements fully correspond to this category with no apparent discrepancies and the GPDR's requirements fairly correspond to this category with minor discrepancies. In terms of the "Risk Assessment" category of the NIST CSF Identify Function, the requirements of CA and NISD fairly correspond to this category with minor discrepancies. About the "Risk Management Strategy" category of the NIST CSF Identify Function, the NISD's requirements fairly correspond to this category with minor discrepancies. As for the "Supply Chain Risk Management" category of the NIST CSF Identify Function, the requirements of the GDPR and NISD fairly correspond to this category with minor discrepancies.

Afterwards, the chapter provides the related work, which revealed that, at the time of conducting the study, no previous research work was found that evaluated all four cybersecurity-related laws (i.e., GDPR, NISD, PDPA, CA) against the NIST CSF Identify Function.

Chapter 4. Evaluation of Cybersecurity Risk Management Frameworks

Chapter 4 extends the research work on the cybersecurity risk management frameworks outlined in **Chapter 2** by proposing a methodology for evaluating cybersecurity risk management frameworks, critically evaluating the in-scope cybersecurity risk management frameworks, and by providing a comprehensive analysis of the related work. Thus, this chapter aims to support decision-making when it comes to cybersecurity risk management framework selection and to facilitate pragmatic implementation of cybersecurity programmes by addressing the need for more evaluations of these frameworks relative to each other. **Chapter 4.1** provides the design of the three-phased methodology that is proposed for evaluating the in-scope frameworks (see Figure 4.1).

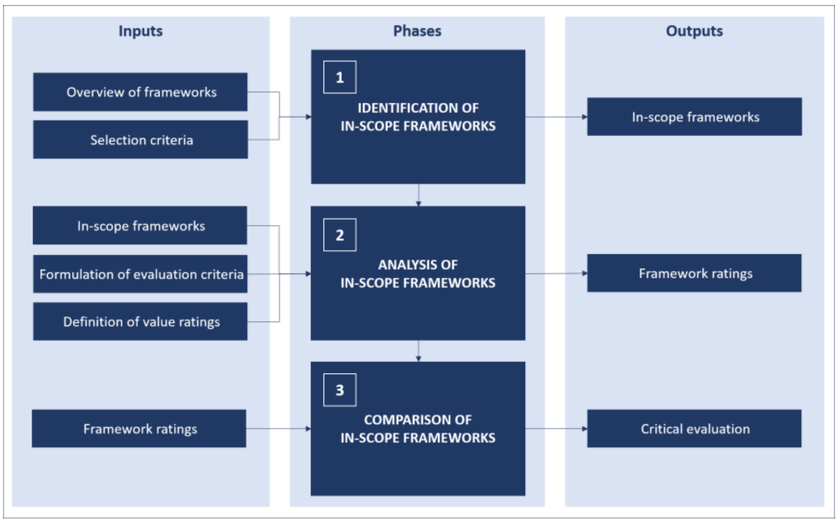

Figure 4.1. The proposed methodology for evaluating the frameworks [Pop20]

With respect to the first phase of the methodology, namely the "identification of in-scope frameworks" phase, this makes use of the overview of the cybersecurity risk management frameworks from Chapter 2.3.1 and the selection criteria of choosing only free of charge frameworks with readily available documentation to determine the in-scope frameworks. Thus, to identify the in-scope frameworks, the selection criteria is applied to the cybersecurity risk management frameworks described in the overview from Chapter 2.3.1.

With respect to the second phase of the methodology, namely the "analysis of in-scope frameworks" phase, this makes use of a proposed hierarchical structure for evaluating frameworks based on Multiple Attribute Decision Making (MADM) approach and the definition of the value ratings to analyse the in-scope cybersecurity risk management frameworks and to determine the framework ratings. With respect to the proposed hierarchical structure (see Figure 4.2), it consists of seven dimensions and thirteen evaluation criteria, where these criteria were formulated to allow a greater characterization of frameworks based on the following dimensions: the definition, purpose, and type of the cybersecurity risk management framework, compatibility with other frameworks and standards or regulatory requirements, key elements pertaining to the risk management process, available supporting documentation, and continuous framework improvement.

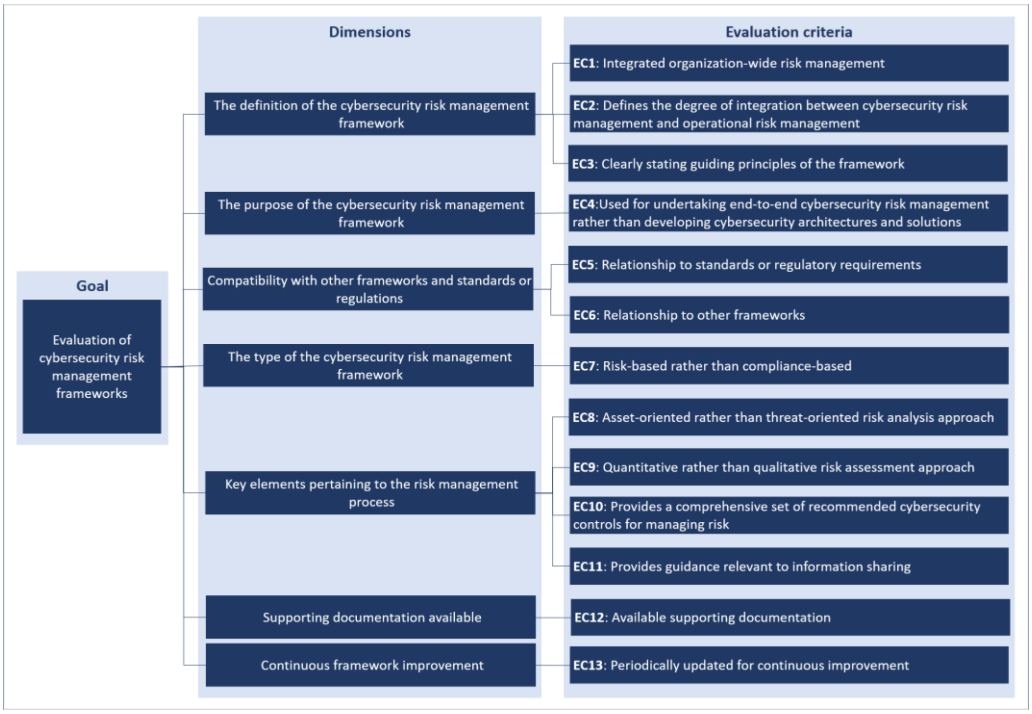

Figure 4.2. The proposed hierarchical structure for evaluating the in-scope frameworks [Pop20]

As for the definition of the value ratings, six linguistic values were defined including "True", "Partly", "Partly*", "Partly**", "False", and "Unclear". Firstly, the "True" value was used to indicate that the evaluation criterion is fully met. Secondly, the "Partly" value was used to indicate that the evaluation criterion applies to a certain extent, but it is not completely met. Thirdly, the "Partly*" value was used to indicate that, where applicable, the evaluation criterion applies both ways. Fourthly, the "Partly**" value was used to indicate that the evaluation criterion applies subject to certain accessibility constraints. Fifthly, the "False" value was used to indicate that the "as-is" criterion is not being met. Sixthly and finally, the "Unclear" value was used to indicate that the corresponding value for the evaluation criterion cannot be precisely set to any of the other five values previously described as the required information is not clearly specified. Thus, to determine the framework ratings, the analysis of the in-scope frameworks involved assigning linguistic value ratings to each of the evaluation criteria for each of the in-scope frameworks to indicate the extent to which in-scope frameworks meet specific evaluation criteria.

With respect to the third phase of the methodology, namely the "comparison of in-scope frameworks" phase, this makes use of the framework ratings resulted from the second phase of the proposed methodology to establish the differences and similarities between the in-scope cybersecurity risk management frameworks.

Then, **Chapter 4.2** provides the critical evaluation of the in-scope cybersecurity risk management frameworks. Hence, there were eight cybersecurity risk management frameworks identified as in scope, namely the NIST's Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF), NIST's Unified Information Security Framework (NIST UISF), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Factor Analysis of Information Risk framework (FAIR), Sherwood Applied Business Security Architecture (SABSA), MITRE's Cyber Resiliency Engineering Framework (MITRE CREF), AICPA's Cybersecurity Risk Management Reporting Framework (AICPA), and CIS Controls version 7 framework (CIS).

Furthermore, the critical evaluation of these frameworks is outlined together with the findings which offer a consolidated characterization of the in-scope cybersecurity risk management frameworks and emphasize similarities and differences between them through the thirteen evaluation criteria of the proposed evaluation methodology. Hence, about the EC1 (i.e, "Integrated organization-wide risk management") evaluation criterion, this is fully met by the NIST CSF, NIST UISF, and SABSA frameworks and it is not met by the OCTAVE, FAIR, AICPA, and CIS frameworks. About the EC2 (i.e., "Defines the degree of integration between cybersecurity risk management and operational risk management") evaluation criterion, this is fully met by NIST CSF, SABSA, and CIS frameworks and it is not met by the remaining frameworks. About the EC3 (i.e., "Clearly stating guiding principles of the framework") evaluation criterion, this is fully met by the OCTAVE, SABSA, MITRE CREF, AICPA, and CIS frameworks and it is not met by the FAIR framework. About the EC4 (i.e., "Used for undertaking end-to-end cybersecurity risk management rather than developing cybersecurity architectures and solutions") evaluation criterion, this is fully met by the NIST CSF and NIST UISF frameworks and it applies both ways to the SABSA framework. About the EC5 (i.e., "Relationship to standards or regulatory requirements") and EC6 (i.e., "Relationship to other frameworks") evaluation criteria, these are fully met by all in-scope cybersecurity risk management frameworks. About the EC7 (i.e., "Risk-based rather than compliance-based") evaluation criterion, this is fully met by the NIST CSF, NIST UISF, OCTAVE, FAIR, SABSA, and MITRE CREF, it applies both ways to the CIS framework, and it is not met by the AICPA framework. About the EC8 (i.e., "Asset-oriented rather than threat-oriented risk analysis approach") evaluation criterion, this is fully met by the OCTAVE, FAIR, SABSA, and AICPA frameworks, it applies both ways to the CIS framework, and it is not met by the NIST UISF framework. About the EC9 (i.e., "Quantitative rather than qualitative risk assessment approach") evaluation criterion, this is fully met by the FAIR framework, it applies both ways to the SABSA framework, and it is not met by the NIST UISF, OCTAVE, and CIS frameworks. About the EC10 (i.e., "Provides a comprehensive set of recommended cybersecurity controls for managing risk") evaluation criterion, this is fully met by the NIST UISF, OCTAVE, SABSA, AICPA, and CIS frameworks and it is not met by the FAIR framework. About the EC11 (i.e., "Provides guidance relevant to information sharing") evaluation criterion, this is fully met by the NIST CSF, NIST UISF, SABSA, MITRE CREF, and AICPA frameworks and it is not met by the OCTAVE and FAIR frameworks. About the EC12 (i.e., "Available supporting documentation – procedures, templates, methods, case studies, etc.") evaluation criterion, this is fully met by the NIST CSF, NIST UISF, OCTAVE, and CIS frameworks. As for the EC13 (i.e., "Periodically updated for continuous improvement") evaluation criterion, this is fully met by all in-scope cybersecurity risk management frameworks, except the OCTAVE framework.

Afterwards, **Chapter 4.3** provides the related work for the evaluation of the cybersecurity risk management frameworks and the related work is discussed by looking at the scope of previous research works and by considering the approach adopted by these works to address the scope. With respect to the scope of previous research works, the related works were mainly focused on evaluations with a narrower scope (i.e., fewer frameworks being addressed, limited to a specific focus area) or on evaluations with a partly different scope (i.e., addressing best-practices irrespective of types, merely focusing on risk assessment / risk management methodologies / methods). With respect to the approach adopted by related works to address the scope, four types of approach were identified. These types include outlining strenghts and weaknesses, comparison based on the structure of the risk assessment / risk management process, comparison based on defined evaluation criteria, and feature-by-feature comparison. Thus, the analysis revealed that the previous related studies neither have broader scope nor they focus exclusively on frameworks.

Chapter 5. IoT Security Risk Management Strategy Reference Model (IoTSRM2)

Chapter 5 extends the research work on the IoT security best practices outlined in **Chapter 2** by proposing a methodology for developing the IoT security risk management strategy reference model, developing the proposed IoT security risk management strategy reference model (IoTSRM2), critically evaluating selected informative references of the IoTSRM2, and providing a comprehensive analysis of the related work for the IoTSRM2 based on eight evaluation criteria. Thus, by addressing the need for a reference model for IoT security risk management strategy, this chapter aims to support practitioners from organizations embracing IoT technologies to formulate or reframe their IoT security risk management strategies and achieve secure Internet of Things (IoT) adoption, and to support fellow researchers from academia that seek to explore the topic of IoT security risk management strategy as part of their research works.

Chapter 5.1 describes the three-phased methodology for developing the proposed IoT security risk management strategy reference model (IoTSRM2) by describing the nine steps of the methodology and their associated outputs (see Figure 5.1).

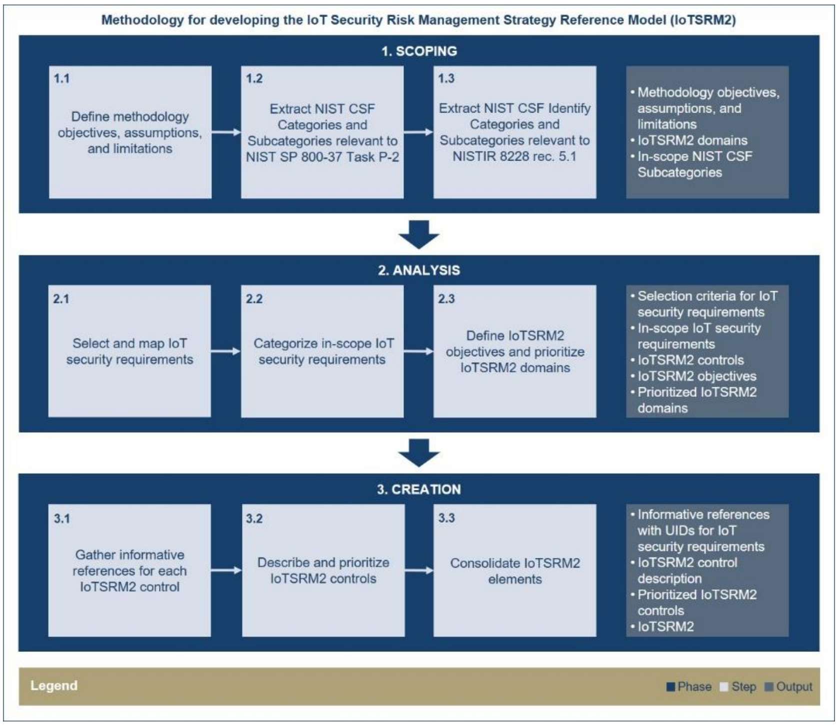

Figure 5.1. The proposed three-phased methodology for developing the IoTSRM2 [Pop+21a]

With respect to the first phase of the methodology (i.e., the "Scoping" phase) which includes three steps, Step 1.1 involved the definition of the methodology objectives, assumptions, and limitations for developing the IoTSRM2. Then, Step 1.2 involved the identification of the six IoTSRM2 domains. Afterwards, Step 1.3 involved the determination of the in-scope NIST CSF Subcategories. With respect to the second phase of the methodology (i.e., the "Analysis" phase) which includes three steps, Step 2.1 involved the definition of criteria for selecting the IoT security requirements from the 25 selected IoT security best practices (see **Chapter 2**), and the mapping of the selected IoT security requirements against the in-scope NIST CSF Subcategories to determine the in-scope IoT security requirements. Aftewards, Step 2.2 involved the categorization of the resulting in-scope IoT security requirements to allow the determination of the IoTSRM2 controls. Next, Step 2.3 involved the definition of each IoTSRM2 objective based on the corresponding in-scope NIST CSF Subcategory and IoTSRM2 controls, and the prioritization of the IoTSRM2 domains based on their corresponding number of IoTSRM2 objectives. Finally, with respect to the third phase of the methodology (i.e., the "Creation" phase) which includes three steps, Step 3.1 involved for each IoTSRM2 control, the collection and documentation of the corresponding informative references together with the applicable unique identifiers of in-scope IoT security requirements. Then, Step 3.2 involved the description of the IoTSRM2 controls in a consistent manner following the levels of detail for controls based on the target information granularity, namely the control description had to include the expected IoT security related activities/actions from IoT adopters, integration points for the expected IoT security related activities/actions with the cybersecurity programs of IoT adopters, and IoT security related activities/actions of IoT suppliers that govern their postmarket activities and that IoT adopters should expect from them. In addition, this step involved the prioritization of the IoTSRM2 controls for each IoTSRM2 objective based on their corresponding adjusted weights which were determined using Equations (5.1) and (5.2). Hence, Equation (5.1) allowed the determination of the IoTSRM2 control weights by taking into account the average in-scope IoT security requirements per an applicable informative reference and the number of in-scope IoT security requirements relative to the 25 selected IoT security best practices for the control in question. In this equation, x_{ijk} represents the controls of the x_{ij} objectives corresponding to the x_i domains of the IoTSRM2, $R(x_{ijk})$ represents the number of in-scope IoT security requirements applicable for each of the x_{ijk} controls of each of the x_{ij} objectives of each of the x_i domains of IoTSRM2, $I(x_{ijk})$ represents the number of informative references applicable for each of the x_{ijk} controls of each of the x_{ij} objectives of each of the x_i domains of IoTSRM2, p represents the number of selected IoT security best practices (see Chapter 2.4), C represents the cardinality of the set of domains x_i, C_i represents the cardinalities of the sets of objectives x_{ij} of each domain from the the set of domains x_i, and n_{ij} represents the number of IoTSRM2 controls corresponding to each objective of the set of objectives x_{ij}.

$$\text{Weight }(x_{ijk}) = \frac{R(x_{ijk})}{I(x_{ijk})} + \frac{R(x_{ijk})}{p}\ , \tag{5.1}$$

$$\text{where } C=|x_i|,\ i=[1..C],\ C_i=|x_{ij}|,\ j=[1..C_i],\ k=[1..n_{ij}]$$

Then the resulting control weights were adjusted using Equation (5.2) to ensure normalization of values:

$$\text{Adjusted weight }(x_{ijk}) = \frac{1}{\sum_1^C C_q} * \frac{\text{Weight }(x_{ijk})}{\sum_{s=1}^{n_{ij}} \text{Weight }(x_{ijs})} * 100\%\ , \tag{5.2}$$

$$\text{where } i=[1..C],\ j=[1..C_i],\ k=[1..n_{ij}], \sum_{i=1}^{C}\sum_{j=1}^{C_i}\sum_{k=1}^{n_{ij}} \text{Adjusted weight }(x_{ijk})=100\%$$

Finally, Step 3.3 involved the consolidation of the IoTSRM2 elements to showcase the proposed IoTSRM2.

Subsequently, **Chapter 5.2** presents the proposed IoTSRM2 which consists of six domains, 16 objectives, and 30 controls for IoT adopters from any sector, which should be addressed by both IoT adopters and IoT suppliers. First, the chapter provides an illustrative overview of the proposed IoTSRM2 (see Figure 5.2).

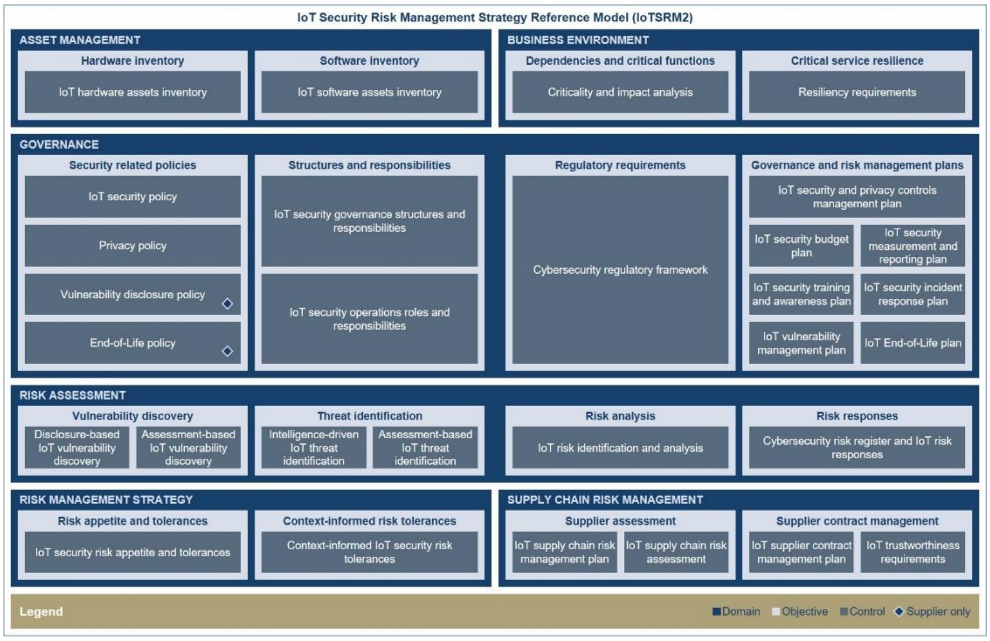

Figure 5.2. The proposed IoTSRM2 [Pop+21a]

Then, for each informative reference of the proposed IoTSRM2, this chapter provides the total number of unique in-scope IoT security requirements mapped to the IoTSRM2 controls, and it indicates whether the informative reference resulted in being among the informative references that are the most relevant to IoT security risk management strategy. Next, for each IoTSRM2 domain, the chapter provides the IoTSRM2 objectives, and, for each IoTSRM2 objective, it describes the IoTSRM2 controls in line with the target information granularity, and it provides, among others, the prioritization of IoTSRM2 controls based on their adjusted weights, which were determined using the Equations (5.1) and (5.2).

Afterwards, **Chapter 5.3** provides the critical evaluation of selected informative references of IoTSRM2 based on their percentage-wise linkage to IoTSRM2, which structured in seven parts, namely in the overall evaluation of selected informative references and the individual evaluations of selected informative references for each IoTSRM2 domain. In this respect, from the 25 informative references of IoTSRM2, seven informative references (i.e., Refs. [Age20a], [CSA19a], [ENI18b], [ENI20a], [IoT16], [IoT20a], and [NIS20a]) were selected for the evaluation as these resulted in being the most relevant to IoT security risk management strategy based on the fulfilment of the two inclusion criteria and two conditions, namey to include the informative references that are the most focused on IoT security risk management strategy and those that are the most applicable to the proposed IoTSRM2, so that the total number of the IoT security requirements applicable to IoTSRM2 of the selected unique informative references to amount to at least half of the total number of the IoT security requirements applicable to IoTSRM2 of all 25 informative references. Hence, with respect to the overall evaluation of selected informative references, for instance, the findings revealed that Ref. [ENI18b] has the strongest links to IoTSRM2 among all 25 informative references and that Ref. [IoT16] is the least linked to IoTSRM2 among the selected informative references (see Figure 5.3).

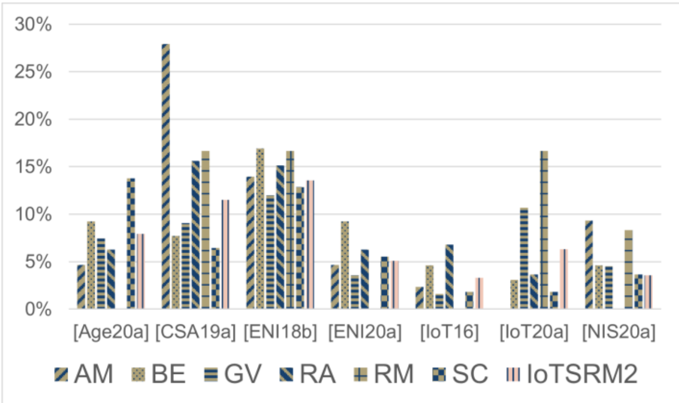

Figure 5.3. Percentage-wise evaluation of selected informative references of IoTSRM2 [Pop+21a]

Moreover, among others, the findings revealed that the majority of the selected informative references are the most focused on the "Governance" domain, and they are the least focused on the "Risk Management Strategy" domain (see Figure 5.4).

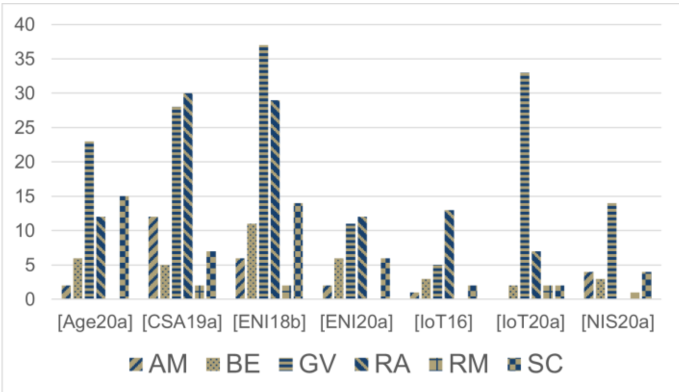

Figure 5.4. Evaluation of selected informative references of IoTSRM2 [Pop+21a]

Then, with respect to the individual evaluations of selected informative references for each IoTSRM2 domain, firstly, about the "Asset Management" domain, the findings revealed, among others, that Ref. [CSA19a] is the most linked to and Ref. [IoT20a] is the least linked to this domain among the selected informative references. Secondly, about the "Business Environment" domain, the findings revealed, among others, that Ref. [ENI18b] is the most linked to and Ref. [IoT20a] is the least linked to this domain among the selected informative references. Thirdly, about the "Governance" domain, the findings revealed, among others, that Ref. [ENI18b] is the most linked to and Ref. [IoT16] is the least linked to this domain among the selected informative references. Fourthly, about the "Risk Assessment" domain, the findings revealed, among others, that Ref. [CSA19a] is the most linked to and Ref. [NIS20a] is the least linked to this domain among the selected informative references. Fifthly, about the "Risk Management Strategy" domain, the findings revealed, among others, that Refs. [CSA19a], [ENI18b], and [IoT20a] are the most linked to and Refs. [IoT16], [ENI20a], and [Age20a] are the least linked to this domain among the selected informative references. Sixthly and finally, about the "Supply Chain Risk Management" domain, the findings revealed, among others, that Ref. [Age20a] is the most linked to and Refs. [IoT20a] and [IoT16] are the least linked to this domain among the selected informative references [Pop21].

Further, **Chapter 5.4** outlines the related work. First, it highlights the absence of research works that exclusively focus on IoT security risk management strategy. Then, it discusses the previous studies that focus on the state of the art or overviews of IoT security best practices, relative to IoTSRM2. Furthermore, to compare the proposed IoTSRM2 with related IoT security best practices, the chapter discusses the IoTSRM2 and the 25 selected IoT security best practices based on eight evaluation criteria and three types of applicability to each evaluation criterion (i.e., the evaluation criterion fully applies, the evaluation criterion applies to a certain extent, but not fully, and the "as-is" evaluation criterion does not apply). Hence, about the E1 (i.e., "Focus on strategic IoT security practices over technical IoT security practices") evaluation criterion, this fully applies to seven informative references and the IoTSRM2 and applies to a certain extent, but not fully, to ten informative references. About the E2 (i.e., "Methodology for developing the recommended IoT security requirements / controls is clearly described") evaluation criterion, this fully applies to seven informative references and the IoTSRM2 and applies to a certain extent, but not fully, to four informative references. About the E3 (i.e., "Mapping of IoT security requirements / controls to NIST CSF's Categories and Subcategories") evaluation criterion, this fully applies to the IoTSRM2 and applies to a certain extent, but not fully, to two informative references. About the E4 (i.e., "Clearly indicate for each IoT security requirement / control expected IoT security actions / activities from IoT suppliers of the target audience") evaluation criterion, this fully applies to the IoTSRM2 and applies to a certain extent, but not fully, to ten informative references. About the E5 (i.e., "Provides integration points with the cybersecurity program as part of each IoT security requirement / control") evaluation criterion, this fully applies to the IoTSRM2 and applies to a certain extent, but not fully, to four informative references. About the E6 (i.e., "Mapping of relevant IoT security best practices with unique identifiers to each recommended IoT security requirement / control") evaluation criterion, this fully applies to two informative references and the IoTSRM2 and applies to a certain extent, but not fully, to eleven informative references. About the E7 (i.e., "Prioritization of the recommended IoT security requirements / controls") evaluation criterion, this fully applies to three informative references and the IoTSRM2 and applies to a certain extent, but not fully, to four informative references. Finally, about the E8 (i.e., "Provides statistics for the mapping of informative references") evaluation criterion, this fully applies to one informative reference and the IoTSRM2 and it does not apply to the remaining informative references.

Chapter 6. Application of an IoTSRM2-Based Survey

Chapter 6 extends the research work on the IoT Security Risk Management Strategy Reference Model (IoTSRM2) outlined in **Chapter 5** by outlining 14 research questions for the IoTSRM2-based survey study, proposing a survey methodology for addressing the research questions, presenting the survey results following the analysis of the survey responses of leaders from industries and governments from around the world, and providing a comprehensive analysis of the related work for the IoTSRM2-based survey study using seven evaluation criteria. Thus, by addressing the need for research works that focus on determining the current state of IoT security risk management strategies in organizations, this chapter aims to support IoT security practitioners from industries and governments to establish the current state of their IoT security risk management strategies when benchmarked against their peers and in turn to enable them to enhance these strategies for matching or outrunning the strategies of their peers.

First, **Chapter 6.1** enumerates the 14 research questions for the IoTSRM2-based survey study and provides a reading map for the research questions (see Figure 6.1). The 14 research questions are the following:

- **RQ1:** What is the overall tendency of the IoT security risk management strategies of the surveyed organizations to meet or deviate from the IoTSRM2 controls?
- **RQ2:** What is the IoTSRM2 compliance score of each of the surveyed organizations?
- **RQ3:** Which is the top organization type for the surveyed organizations by survey respondents?
- **RQ4.a:** Which is the top industry sector for the surveyed organizations by survey respondents?

- **RQ4.b:** Which is the top industry sector for the surveyed organizations of the top organization type by survey respondents?
- **RQ5.a:** What is the overall average IoTSRM2 compliance score of the surveyed organizations for each IoTSRM2 control?
- **RQ5.b:** What is the overall average IoTSRM2 compliance score of the surveyed organizations of the top organization type for each IoTSRM2 control?
- **RQ5.c:** What is the overall average IoTSRM2 compliance score of the surveyed organizations from the top industry sector of the top organization type for each IoTSRM2 control?
- **RQ6.a:** Which is the top position level of the survey respondents for the surveyed organizations by survey respondents?
- **RQ6.b:** Which is the top position level of the survey respondents for the surveyed organizations of the top organization type by survey respondents?
- **RQ6.c:** Which is the top position level of the survey respondents for the surveyed organizations from the top industry sector of the top organization type by survey respondents?
- **RQ7.a:** Which is the top region for the surveyed organizations by survey respondents?
- **RQ7.b:** Which is the top region for the surveyed organizations of the top organization type by survey respondents?
- **RQ7.c:** Which is the top region for the surveyed organizations from the top industry sector of the top organization type by survey respondents?

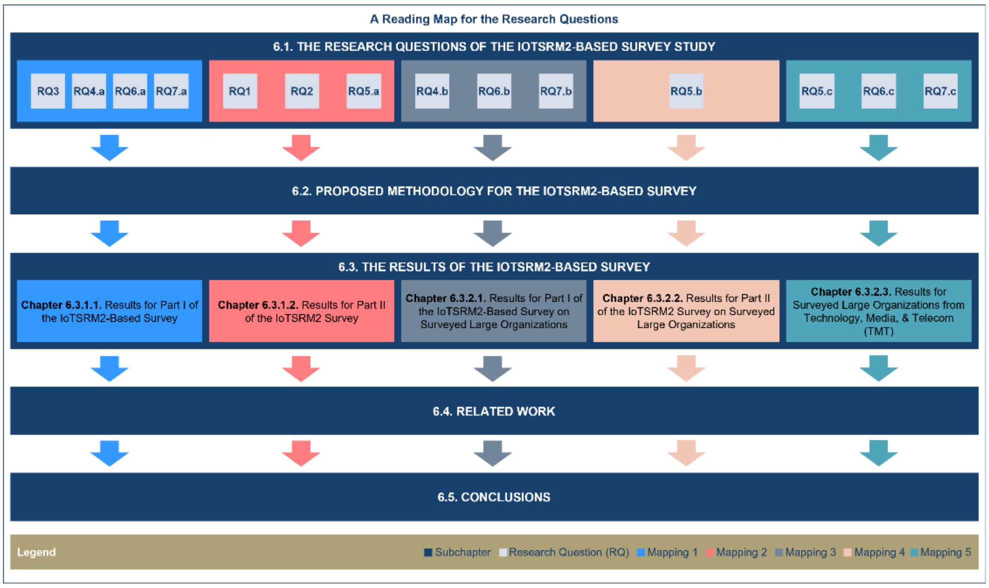

Figure 6.1. A reading map for the research questions [Pop+21b]

Then, **Chapter 6.2** describes the proposed three-phased survey methodology for addressing the research questions, by describing the nine steps of this methodology and their associated outputs (see Figure 6.2). With respect to the first phase of the survey methodology (i.e., the "Plan and Create" phase) which includes three steps, Step I.1 involved the definition of the methodology objectives, survey assumptions, and limitations. Then, Step I.2 involved the development of the questionnaire for the IoTSRM2-based survey, which is structured in part I and part 2 including five screening and background questions with possible answers and 30 IoTSRM2-related questions with possible answers (i.e., "No, to a great extent", "No, to a certain extent", "Yes, to a certain extent", "Yes, to a great extent"), respectively. Afterwards Step I.3 involved the design and creation of the survey based on the principles for designing web questionnaires developed by Dillman et al. (1999) [Dil+99], along with the development of the survey analysis plan. With respect to the second phase of the survey methodology (i.e., the "Launch and Run" phase) which includes three steps, Step II.1 involved the identification of the target survey respondents for the sampling frame, and the creation and submission of participation requests to target respondents for the IoTSRM2-based survey. Aftewards, Step II.2 involved the submission of a combination of reminders including private messages and social media posts about the IoTSRM2-based survey. Next, Step II.3 involved the export of all survey responses from SurveyMonkey to Excel once the survey ended.

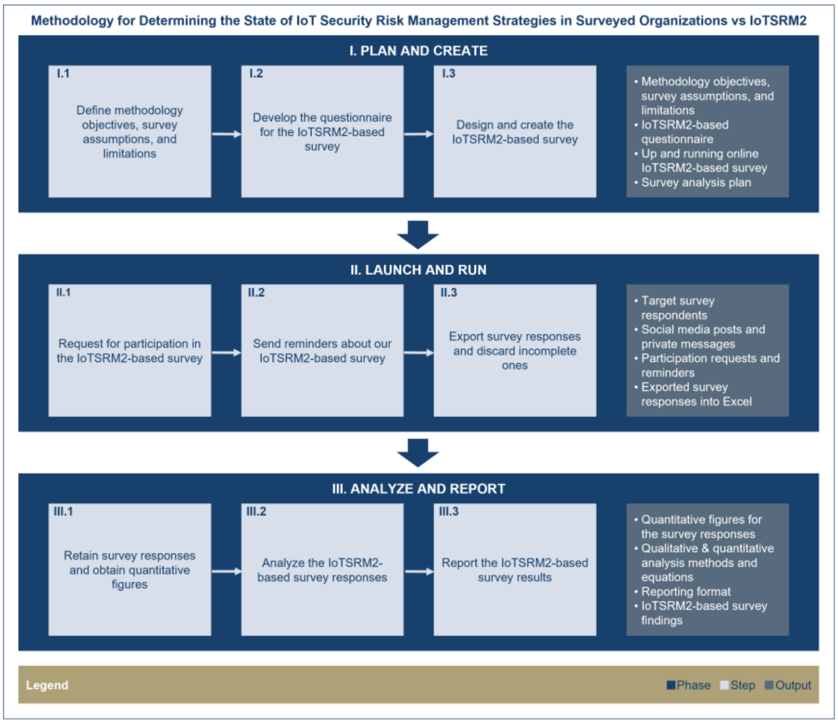

Figure 6.2. The proposed three-phased survey methodology [Pop+21b]

Finally, with respect to the third phase of the survey methodology (i.e., the "Analyze and Report" phase) which includes three steps, Step III.1 involved the retention of the exported survey responses in their original form and the conversion of the qualitative IoTSRM2-related responses into quantitative figures using Equation (6.1), where Q_j represents the 30 IoTSRM2-related questions, $Response_i(Q_j)$ represents the responses of the survey respondents to the IoTSRM2-related questions, R_{ij} represents the percentage scores corresponding to survey respondents for the IoTSRM2-related questions (see Step I.2), and K represents the cardinality of the survey respondents:

$$\text{Convert}\ (Response_i(Q_j))=R_{ij},$$

$$\text{where } R_{ij}=\begin{cases} 0, & Response_i(Q_j)=\text{"No, to a great extent"} \\ 30\%, & Response_i(Q_j)=\text{"No, to a certain extent"} \\ 70\%, & Response_i(Q_j)=\text{"Yes, to a certain extent"} \\ 100\%, & Response_i(Q_j)=\text{"Yes, to a great extent"} \end{cases} \tag{6.1}$$

$$i=[1..K],\ j=[6..35],\ \text{and } K=|\text{survey respondents}|$$

Then, Step III.2 involved the analysis of all survey responses across three groups of surveyed organizations (see Figure 6.3). Thus, with respect to the analysis of the survey responses for the part I of the IoTSRM2-based survey, first, the I.A analysis aimed to address the RQ6.a, RQ6.b, and RQ6.c research questions. Second, the I.B analysis aimed to address the RQ3 research question. Third, the I.C analysis aimed to address the RQ4.a and RQ4.b research questions. Finally, the I.D analysis aimed to address the RQ7.a, RQ7.b, and RQ7.c research questions.

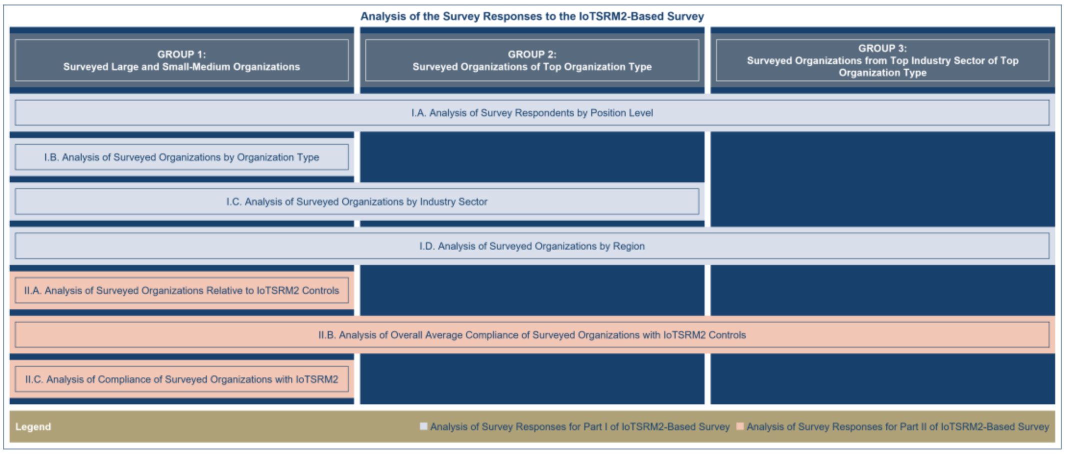

Figure 6.3. Outline of the analysis of the responses to the IoTSRM2-based survey [Pop+21b]

Furthermore, with respect to the analysis of the survey responses for the part II of the IoTSRM2-based survey, first, the II.A analysis aimed to address the RQ1 research question. This analysis involved comparing the percentage of survey responses of "Yes, to a certain extent" and "Yes, to a great extent" against the percentage of survey responses of "No, to a great extent" and "No, to a certain extent" for each IoTSRM2-related question. Second, the II.B analysis aimed to address the RQ5a, RQ5.b and RQ5.c research questions. This analysis involved computing, for each IoTSRM2 control and related question for each of the three groups of surveyed organizations, the overall average compliance score using the Equations (6.2) and (6.3) based on the survey responses and the corresponding adjusted control weight. In Equation (6.2), $\text{Compliance}_i(C_j)$ represents the compliance scores of the surveyed organizations with the IoTSRM2 controls, C_j represents the IoTSRM2 controls that correspond to the IoTSRM2-related questions, $\text{Adjusted weight}\ (C_j)$ represents the adjusted weights corresponding to the IoTSRM2 controls, and R_{ij} and K are described above (see Step III.1).

$$\text{Compliance}_i(C_j)=R_{ij}*\text{Adjusted weight}\ (C_j)$$
$$\text{where } i=[1..K],\ j=[6..35], \text{ and } K=|\text{survey respondents}| \tag{6.2}$$

Then, the overall average compliance scores were computed using Equation (6.3), where L_k represents the cardinality of the survey respondents for the Group k of surveyed organizations (i.e., the Group 1, Group 2, and Group 3), and $\text{Compliance}_i(C_j)$ and C_j are described above.

$$\text{Overall average compliance}\ (C_j)=\frac{\sum_{i=1}^{L_k}\text{Compliance}_i(C_j)}{L_k},$$
$$\text{where } i=[1..L_k],\ j=[6..35],\ k=[1..3],$$
$$\text{and } L_k=|\text{survey respondents for Group k of surveyed organizations}| \tag{6.3}$$

Third, the II.C analysis aimed to address the RQ2 research question. This analysis involved determining, for each of the surveyed organizations, the IoTSRM2 compliance score using Equation (6.4), where $\text{IoTSRM2 compliance score}_i$ represents the IoTSRM2 compliance scores of the surveyed organizations, and $\text{Compliance}_i(C_j)$, C_j, and K are described above.

$$\text{IoTSRM2 compliance score}_i=\sum_{j=6}^{35}\text{Compliance}_i(C_j),$$
$$\text{where } i=[1..K],\ j=[6..35],\ K=|\text{survey respondents}| \tag{6.4}$$

Furthermore, this step involved the development of a naming convention for the surveyed organizations to facilitate the II.C analysis and to distinguish between them easier given the anonymous nature of the IoTSRM2-based survey.

Ultimately, Step III.3 provided the reporting structure for the IoTSRM2-based survey findings and involved the reporting of the IoTSRM2-based survey results for each of the three groups of surveyed organizations outlined in Step III.2.

Subsequently, **Chapter 6.3** presents the IoTSRM2-based survey results for the three groups of surveyed organizations (i.e., the surveyed large and small-medium organizations, the surveyed large organizations, the surveyed large TMT organizations) that show the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2.

Hence, about the results for all surveyed organizations, first, these results revealed that the "C-level executive and/or board member" and "Consulting practice leader and/or principal" position levels are the top position levels of the survey respondents for these organizations. Second, the IoTSRM2-based survey results revealed that the "Large Organization" category is the top organization type for these organizations. Third, IoTSRM2-based survey results showed that the "Technology, Media, & Telecom (TMT)" industry sector is the top industry sector for these organizations. Fourth, these results showed that the "North/South America" region is the top region for these organizations. Fifth, about the overall tendency of the IoT security risk management strategies of these organizations relative to the IoTSRM2 controls, the findings revealed that 18 IoTSRM2 controls and related questions correspond to the "No, to a certain and great extent" group of answer choices and the other 12 IoTSRM2 controls and related questions correspond to "Yes, to a certain and great extent" group of answer choices (see Figure 6.4). For instance, these findings suggested, among others, that most organizations do best in the "Resiliency requirements" control and they do worst in the "IoT security training and awareness plan" and "IoT End-of-Life plan" controls.

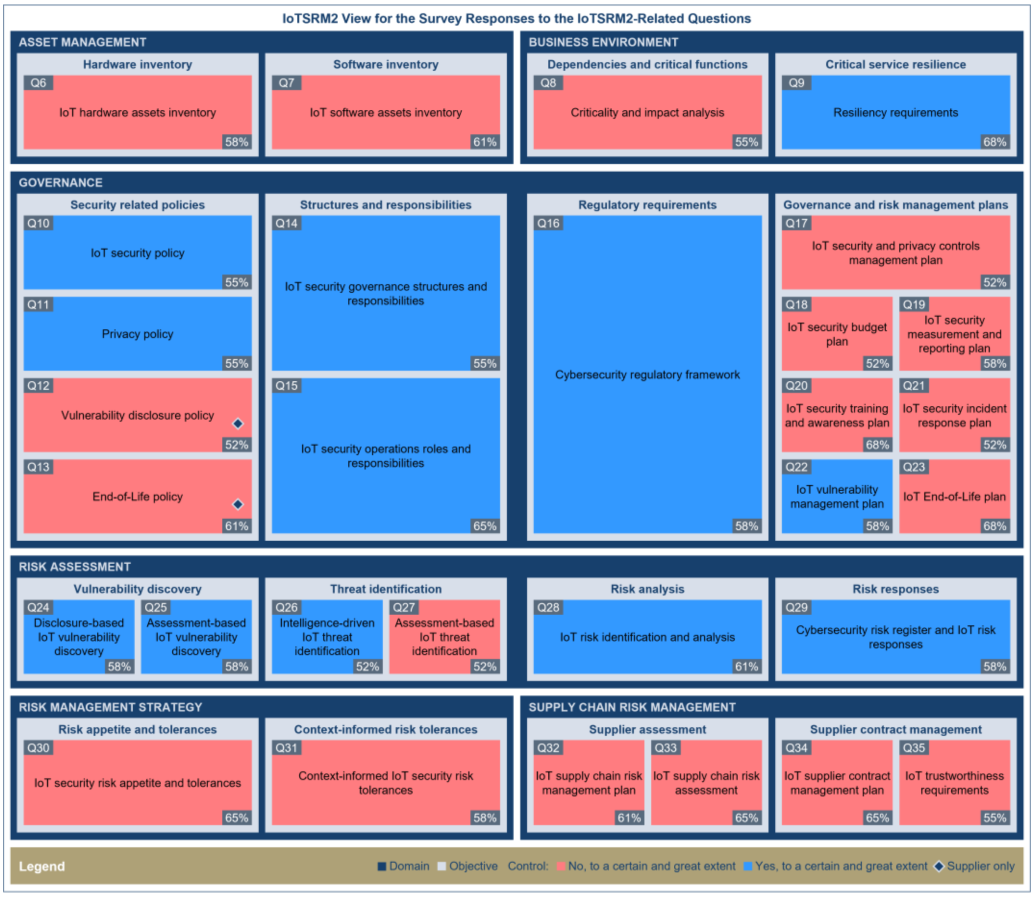

Figure 6.4. IoTSRM2 overview for the responses to the IoTSRM2-based survey [Pop+21b]

Then, about the overall average IoTSRM2 compliance score of these organizations for each IoTSRM2 control, the findings revealed that the overall average IoTSRM2 compliance score of less than 50% and greater than or equal to 50% correspond to 19 and 11 IoTSRM2 controls (see Figure 6.5), respectively. For instance, these findings showed, among others, that most organizations do best in the "Resiliency requirements" control and they do worst in the "IoT security training and awareness plan" and "IoT supplier contract management plan" controls.

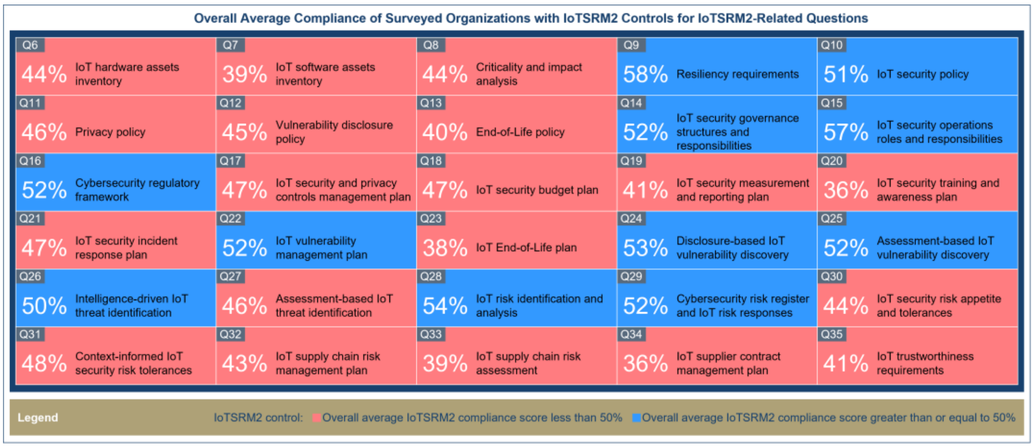

Figure 6.5. Overall average compliance with IoTSRM2 controls based on the survey responses [Pop+21b]

As for the IoTSRM2 compliance score of each of these organizations, the IoTSRM2-based survey results revealed that the IoTSRM2 compliance score of less than 50% and greater than or equal to 50% correspond to 19 and 12 surveyed organizations (see Figure 6.6), respectively. For instance, these findings showed, among others, that the top three highest and lowest IoTSRM2 compliance scores for the surveyed organizations correspond to large (i.e., except for one of them) and small-medium organizations, respectively.

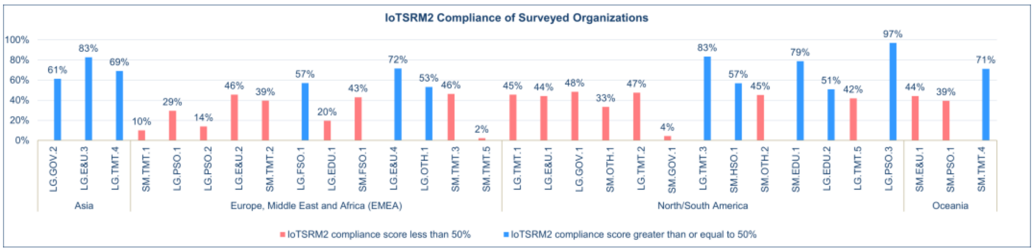

Figure 6.6. The IoTSRM2 compliance of surveyed organizations [Pop+21b]

Furthermore, about the results for the surveyed large organizations, first, these results revealed that the "Consulting practice leader and/or principal" position level is the top position level of the survey respondents for these organizations. Second, the IoTSRM2-based survey results showed that the "Technology, Media, & Telecom (TMT)" industry sector is the top industry sector for these organizations. Third, the IoTSRM2-based survey results showed that the "North/South America" region is the top region for these organizations. Fourth, about the overall average IoTSRM2 compliance score of these organizations for each IoTSRM2 control, the findings revealed that the overall average IoTSRM2 compliance score of less than 50% and greater than or equal to 50% correspond to 10 and 20 IoTSRM2 controls (see Figure 6.7), respectively. For instance, these findings showed, among others, that most organizations do best in the "Resiliency requirements" control and they do worst in the "IoT software assets inventory" control.

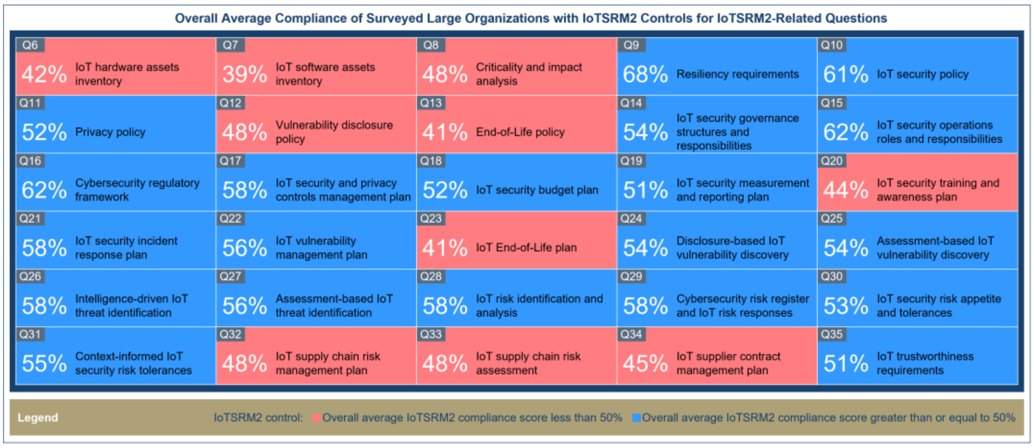

Figure 6.7. Overall average compliance with IoTSRM2 controls based on the survey responses for large organizations [Pop+21b]

Furthermore, about the results for the surveyed large TMT organizations, first, the IoTSRM2-based survey results revealed that the "Consulting practice leader and/or principal" and "C-level executive and/or board member" position levels are the top position levels of the survey respondents for these organizations. Second, the findings showed that the "North/South America" region is the top region for these organizations. Third, about the overall average IoTSRM2 compliance score of these organizations for each IoTSRM2 control, the findings revealed that the overall average IoTSRM2 compliance score of less than 50% and greater than or equal to 50% correspond to 9 and 21 IoTSRM2 controls (see Figure 6.8), respectively. For instance, these IoTSRM2-based survey results showed, among others, that most organizations do best in the "IoT security policy" control and they do worst in the "Criticality and impact analysis" control.

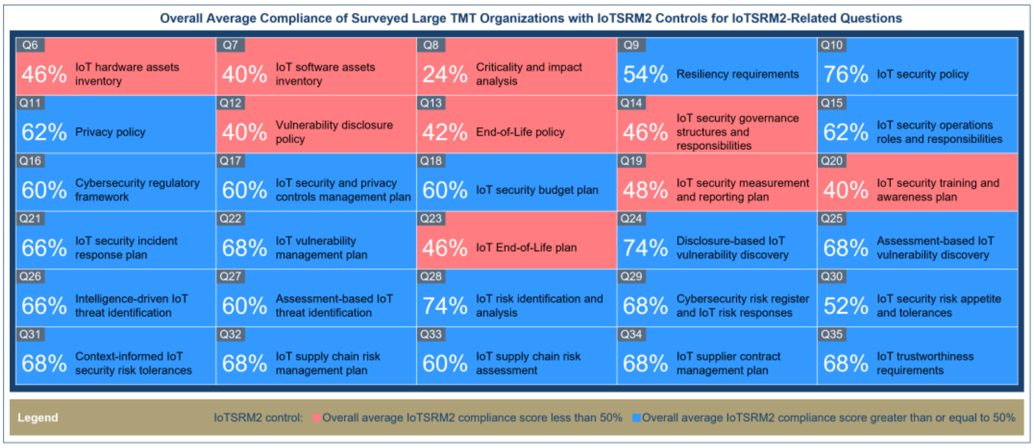

Figure 6.8. Overall average compliance with IoTSRM2 controls based on the survey responses for large TMT organizations [Pop+21b]

Then, **Chapter 6.4** outlines the related work. First, it highlighted the absence of research studies that exclusively focus on determining the current state of IoT security risk management strategies in organizations. Second, it provides the 12 related research studies which were selected based on three selection criteria and one condition, namely to include English written interview-, survey-, or experiment-based research works from both academia and industry, that address the IoT security risk management strategy in organizations at least to a certain extent. Third, it discusses the IoTSRM2-based survey study in relation to the selected related studies using seven evaluation criteria based on the proposed methodology and using three types of applicability to each evaluation criterion (i.e., the evaluation criterion fully applies, the evaluation criterion applies to a certain extent, and the "as-is" evaluation criterion does not apply). Hence, about the E1 (i.e., "The research study is focused on determining the current state of IoT security risk management strategies in organizations") evaluation criterion, this fully applies to the IoTSRM2-based survey study and applies to a certain extent to 12 related studies. About the E2 (i.e., "The methodology for achieving the intended purpose of the research study is clearly described") evaluation criterion, this fully applies to one related study and the IoTSRM2-based survey study and applies to a certain extent to five related studies. About the E3 (i.e., "The underlying design best practice of the research method of the methodology, is clearly documented") evaluation criterion, this fully applies to the IoTSRM2-based survey study and applies to a certain extent to one related study. About the E4 (i.e., "Provides results for organizations of a specific organization size") evaluation criterion, this fully applies to three related studies and the IoTSRM2-based survey study and does not apply to the other related studies. About the E5 (i.e., "Provides results for organizations from a specific industry sector") evaluation criterion, this fully applies to four related studies and the IoTSRM2-based survey study and does not apply to the other related studies. About the E6 (i.e., "The results reveal the level of compliance of each subject with a reference model") evaluation criterion, this fully applies to the IoTSRM2-based survey study and applies to a certain extent to one related study. Finally, about the E7 (i.e., "The findings resemble the results of the IoTSRM2-based survey") evaluation criterion, this fully applies to the IoTSRM2-based survey study and applies to a certain extent to eight related studies.

Chapter 7. Final Conclusions

Chapter 7 presented the final conclusions of this thesis, thesis contributions, and future work. Thus, this thesis presents several contributions which are grouped into three categories: theoretical contributions, theoretical contributions applicable in practice, practical contributions.

First, **the theoretical contributions** are:

- The definition of the „standard", „method", and „methodology" terms to clearly delineate the distinction between them;
- The definition of the „cybersecurity risk management framework" term to enable a common understanding of this term;
- The development of a novel taxonomic hierarchy that classifies IoT security best practices based on their applicability to specific groups of target audience and type of IoT security best practice;
- A comparison of the proposed threat rating method with the related work;
- An analysis of the related work relevant to the evaluation of cybersecurity-related legislations;
- A comprehensive analysis of the related work relevant to the evaluation of cybersecurity risk management frameworks that delved into previous studies with a narrower scope and a partly different scope;
- A comparative analysis of the related work for the proposed reference model based on a proposed set of evaluation criteria;
- A comparative analysis of the related work for this IoTSRM2-based survey study based on a proposed set of evaluation criteria.

Second, **the theoretical contributions applicable in practice** are:

- The identification, categorization, and description of standards and methodologies relevant to cybersecurity risk management based on the study of the literature on cybersecurity risk management;
- The determination and categorization of current cyber threats into thirteen up-to-date cyber threat categories along with the description of these cyber threat categories based on the investigation of seventeen relevant and well-renowned sources;
- An overview of the cybersecurity-related legislations and regulations pertaining to two cybersecurity areas of statute for three separate jurisdictions;
- The identification, categorization, and description of frameworks relevant to cybersecurity risk management based on the study of the literature on the cybersecurity risk management;
- The identification, classification, and description of IoT security best practices based on the study of literature and the proposed taxonomic hierarchy;
- The design of a novel cyber threat rating method and the creation of a threat rating tool;
- The design of a new method for evaluating selected key cybersecurity-related legislations;
- The design of a three-phased methodology that involves identification, analysis, and comparison of in-scope cybersecurity risk management frameworks;
- The development of a hierarchical structure for evaluating the in-scope cybersecurity risk management frameworks, which includes seven dimensions and thirteen evaluation criteria;

- The definition of six linguistic values for rating the in-scope cybersecurity risk management frameworks against the evaluation criteria;
- The design of a methodology for developing the IoT security risk management strategy reference model based on best practices;
- The design of a methodology for determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2.

Third, **the practical contributions** are:

- The application of the proposed cyber threat rating method to thirteen cyber threat categories for evaluating these cyber threat categories;
- The critical evaluation of the thirteen cyber threat categories based on their possible extents of applicability to cyber harm;
- The critical evaluation of the in-scope cybersecurity-related legislations to establish the degree of commonality between them from the perspective of organizational understanding to managing cybersecurity risk;
- The critical evaluation of eight cybersecurity risk management frameworks based on the proposed evaluation methodology;
- The development of a reference model for IoT security risk management strategy that is suitable for IoT adopters from any sector based on the proposed methodology;
- A critical evaluation of selected informative references of the IoTSRM2 based on their linkage to the proposed reference model;
- The design, creation, testing, and distribution of the IoTSRM2-based survey based on the proposed survey methodology;
- The determination of the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2 by analyzing the survey responses and reporting the IoTSRM2-based survey results.

Selected References

[Age20a] AgeLight LLC. (2020a). *IoT Safety Architecture & Risk Toolkit, version 4.0*. AgeLight LLC. Retrieved February 23, 2021, from https://www.agelight.com/iot

[Agr+18] Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1–15. https://doi.org/10.1093/cybsec/tyy006

[ATK18] A.T. Kearney. (2018). *Rising to the Challenge 2018 Views from the C-Suite An Annual Survey of Global Business Executives*. A.T. Kearney, Inc*.* Retrieved October 3, 2020, from https://www.kearney.com/web/global-business-policy-council/article?/a/2018-views-from-the-c-suite

[CSA19a] CSA. (2019a). *CSA IoT Security Controls Framework*. Cloud Security Alliance. Retrieved May 06, 2020, from https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/

[Dil+99] Dillman, D.A., Tortora, R., & Bowker, D. (1999). *Principles for constructing Web surveys*. Pullman: Washington State University, Social and Economic Sciences Research Center.

[ENI18b] ENISA. (2018b). *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*. The European Union Agency for Cybersecurity. Retrieved July 20, 2020, from https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

[ENI20a] ENISA. (2020a). *Procurement Guidelines for Cybersecurity in Hospitals Good practices for the security of Healthcare services*. The European Union Agency for Cybersecurity. Retrieved January 05, 2021, from https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[Giu+21] Giuca, O., **Popescu, T.M**., Popescu, A.M., Prostean, G., & Popescu, D.E. (2021). A Survey of Cybersecurity Risk Management Frameworks. In V. Balas, L. Jain, M. Balas & S. Shahbazova (Eds.), *Soft Computing Applications. SOFA 2018. Advances in Intelligent Systems and Computing* (Vol. 1221, pp. 240-272). Cham: Springer. https://doi.org/10.1007/978-3-030-51992-6_20

[IoT16] IoTAC, (2016), 'IoT Security Guidelines Ver. 1.0,' [Online], *Japan's IoT Acceleration Consortium*, [Retrieved August 13, 2020], Available: http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf

[IoT20a] IoTSF. (2020a). *IoT Security Compliance Framework Release 2.1*. IoT Security Foundation. Retrieved July 20, 2020, from https://www.iotsecurityfoundation.org/best-practice-guidelines/

[ITU12] ITU-T. (2012). *Overview of the Internet of Things*. ITU Telecommunication Standardization Sector. Retrieved September 05, 2021, from https://www.itu.int/rec/T-REC-Y.2060-201206-I/en

[ITU17] ITU. (2017). *Global Cybersecurity Index (GCI) 2017*. ITU. Retrieved November 19, 2018, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[Nat17] National Academy of Engineering. (2017). *NAE GRAND CHALLENGES FOR ENGINEERING*. National Academy of Engineering. Retrieved May 28, 2019, from http://www.engineeringchallenges.org/challenges/11574.aspx

[NIS18a] NIST. (2018a). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. National Institute of Standards and Technology. Retrieved February 10, 2019, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[NIS20a] NIST. (2020a). *Foundational Cybersecurity Activities for IoT Device Manufacturers*. National Institute of Standards and Technology. Retrieved January 07, 2021, from https://doi.org/10.6028/NIST.IR.8259

[Pop+19a] **Popescu, T.M.**, Popescu, A.M., Prostean, G., & Popescu, D.E. (2019a). Evaluation of legislations from the perspective of organizational understanding to managing cybersecurity risk. In K.S. Soliman (Eds.) *Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020* (pp. 4677-4689). ISBN: 978-0-9998551-2-6.

[Pop+19b] **Popescu, T.M.**, Popescu, A.M., Prostean, G., & Popescu, D.E. (2019b). Cybersecurity Threat Rating Method Based on Potential Cyber Harm', In: Soliman K. S. (Eds.) *Proceedings of the 34th International Business Information Management Association Conference (IBIMA). Vision 2025: Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage* (pp. 5909- 5920). ISBN: 978-0-9998551-3-3.

[Pop20] **Popescu, T.M.** (2020). *Cybersecurity Risk Management* (Ph.D. Report 1). Politehnica University of Timisoara, Timisoara, Romania.

[Pop21] **Popescu, T.M.** (2021). *IoT Security Risk Management* Strategy (Ph.D. Report 2). Politehnica University of Timisoara, Timisoara, Romania.

[Pop+21a] **Popescu, T.M.**, Popescu, A.M., & Prostean, G. (2021a). IoT Security Risk Management Strategy Reference Model (IoTSRM2). *Future Internet*, *13* (6), 148. https://doi.org/10.3390/fi13060148

[Pop+21b] **Popescu, T.M.**, Popescu, A.M., & Prostean, G. (2021b). Leaders' Perspectives on IoT Security Risk Management Strategies in Surveyed Organizations Relative to IoTSRM2. Applied Sciences, 11 (19), 9206. https://doi.org/10.3390/app11199206