applied sciences

MDPI

Article

Leaders' Perspectives on IoT Security Risk Management Strategies in Surveyed Organizations Relative to IoTSRM2

Traian Mihai Popescu [1,*], Alina Madalina Popescu [2] and Gabriela Prostean [1]

[1] Management Department, Faculty of Management in Production and Transportation, Politehnica University of Timisoara, 14 Remus Street, 300191 Timisoara, Romania; gabriela.prostean@upt.ro
[2] PactFlux SRL, 101 Leurda, 215204 Motru, Romania; pampopescu2017@gmail.com
* Correspondence: traian.popescu@student.upt.ro

Abstract: In the COVID-19 and post-pandemic business environment, leveraging robust Internet of Things (IoT) security risk management strategies becomes of particular importance to IoT adopters. Thus, given that no research study was found to exclusively focus on the current state of IoT security risk management strategies in organizations, this article aims to support IoT security practitioners to peer benchmark and enhance their IoT security risk management strategies. In a nutshell, this study relies on a mixed methods research methodology, and its main contribution is the determination of the current state of the IoT security risk management strategies in the surveyed organizations relative to our IoT Security Risk Management Strategy Reference Model (IoTSRM2). Hence, this study entails designing and conducting a survey, analyzing survey responses, and reporting survey results based on our IoTSRM2 and proposed three-phased survey methodology. Furthermore, before discussing the related work, this article provides our survey results for the surveyed large and small-medium organizations, the surveyed large organizations, and the surveyed large Technology, Media, and Telecom (TMT) organizations. For instance, our results reveal that while most surveyed organizations perform IoT risk assessments and focus on IoT infrastructure resilience, they fail in strategizing IoT governance and risk management, among others.

Keywords: Internet of Things; IoT security; cybersecurity; risk management; technology strategy; reference model; survey design; benchmarking; gap analysis; current state assessment

Citation: Popescu, T.M.; Popescu, A.M.; Prostean, G. Leaders' Perspectives on IoT Security Risk Management Strategies in Surveyed Organizations Relative to IoTSRM2. *Appl. Sci.* **2021**, *11*, 9206. https://doi.org/10.3390/app11199206

Academic Editor: Igal M. Shohet

Received: 30 July 2021
Accepted: 1 October 2021
Published: 3 October 2021

1. Introduction

These days, organizations from around the world leverage technological advances at an unprecedented pace [1]. The COVID-19 pandemic has further fueled technical innovations and technological convergence, expedited digital connectivity in and around organizations, and made way for a greater international appetite towards remote everything (e.g., remote work, remote healthcare) [2]. In this context, this pandemic arguably acted as a catalyst for greater critical dependency on internet-based technologies [3] including, inter alia, some of the Internet of Things (IoT) technologies. For instance, throughout the COVID-19 pandemic, IoT has been employed for predicting how the COVID-19 pandemic unfolds, tracking the health conditions of people, monitoring COVID-19 patients, tracking the real-time location of medical equipment, and detecting fraudulent healthcare insurance claims [4]. Moreover, the application of IoT in healthcare was studied as part of a systematic review conducted by Kashani et al. [5]. Besides its application in healthcare, IoT has various application areas, including smart mobility, smart grid, smart home/building, public safety and environment monitoring, industrial processing, smart agriculture, and independent living [6]. Hence, there are numerous research studies that cover individual and various application areas of IoT. With respect to the various application areas of IoT, examples of studies include the comprehensive review conducted by Khanna and Kaur [6] that highlighted, among others, various contributions of researchers in different

areas of applications of IoT, and the comprehensive literature-based survey conducted by Hassan et al. [7] that focused on exploring the applications of IoT in different areas, including healthcare, environmental, commercial, industrial, smart cities, and infrastructural applications. Then, with respect to the individual application areas of IoT, examples of studies include the research works about an advanced IoT-based transportation system for efficient vehicle routing and scheduling in urban areas that described the concept and methodological approach for its development [8], proposed its architecture [9], and demonstrated its use in a case study [10]. Thus, the various application areas of IoT along with the numerous research contributions in different areas of applications of IoT indicate an extensive appetite for leveraging IoT technologies.

Furthermore, the World Economic Forum [11] anticipated an even faster adoption of IoT technologies in the post COVID-19 economy. The prospect of IoT growth over the next few years was also highlighted in the study conducted by Khanna and Kaur [6], which pointed out that the need for greater interaction between various entities and more precise evaluation of sensor data are key drivers for ubiquitous connectivity.

Notwithstanding, the aggressive adoption of and reliance on new network- and internet-connected technologies within organizations broaden their attack surface [12] and heighten their inherent cybersecurity risk through and beyond the coronavirus pandemic. In this context, the COVID-19 crisis may invite more numerous hostile actors to capitalize on cybercrime by targeting vulnerable organizations [13], which in effect makes cybersecurity risk more prevalent. In addition, the projected growth of IoT in the post COVID-19 business environment [11] may further widen the attack surface of organizations and exacerbate their cybersecurity risk through the expansion of IoT security risk. Hence, considering that IoT security risk management is a challenge for organizations [14], having a robust IoT security risk management strategy in place becomes of particular importance [15] through and beyond the COVID-19 pandemic.

In this context, numerous entities around the globe are working on developing mandatory and voluntary IoT security requirements aimed at stimulating industry and government organizations to adopt robust IoT security practices. Hence, on top of the existing cybersecurity-related laws and regulations [16], government and regulatory bodies from around the world work on introducing new laws to increase IoT security. For instance, the U.S. Congress [17] enacted the federal IoT Cybersecurity Improvement Act of 2020, which aims to "establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes", and the UK's Department for Digital, Culture, Media & Sport [18] plans to introduce new laws that regulate the security of consumer IoT devices. Moreover, in response to the IoT security issues and risk, domestic and international standards bodies and industry associations have developed various IoT security codes of practice, standards, guidelines, and frameworks [14].

However, given the absence of a global baseline IoT security standard [11], the issue that the existing IoT security best practices are primarily focused on the more technical aspects [3], and the acute need for better IoT security risk management in organizations [19], the IoT security risk management strategies of industry and government organizations embracing IoT technologies tend to be more fragile than robust [14].

This prevalent absence of robust IoT security risk management strategies in organizations together with the paucity of IoT security risk management reference sources were highlighted in our previous article [14], which revealed the absence of an IoT security risk management strategy reference model. This research problem was addressed by proposing a novel IoT security risk management strategy reference model (IoTSRM2) to support IoT security practitioners from industries and governments to frame or rethink their IoT security risk management strategies [14]. Thus, this article extends on our previous research work [14] and focuses on addressing the proposed future work, namely the undertaking of an IoTSRM2-based survey to determine the current state of IoT security risk management strategies in surveyed organizations relative to our IoTSRM2.

Moreover, considering that, at the time of writing, there is no research study found to exclusively focus on determining the current state of IoT security risk management strategies in surveyed organizations, there is a clear research gap in terms of the existence of such a research study. Thus, the purpose of this research article is to undertake an IoTSRM2-based survey to determine the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2 considering the views of leaders from industries and governments from around the world. Moreover, this research article 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 IoT security risk management strategies of their peers.

Hence, in response to the research gap and the purpose mentioned above, the research questions of this research study 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?

To address the research questions above and achieve the intended outcome of this research study, this article relies on a mixed methods research methodology harnessing both qualitative and quantitative methods. Thus, our research work makes use of quantitative data to complement the qualitative data, which adds value to the outputs of this research and allows the reporting of the IoTSRM2 compliance results. In this context, the outputs of this research work concretize into the main contributions outlined below:

- The design of a methodology for determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2;
- 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 our IoTSRM2-based survey results;
- A comparative analysis of the related work for this IoTSRM2-based survey study based on a set of evaluation criteria.

Beyond this introductory section, the remainder of this article is organized as depicted in Figure 1. Section 2 provides an overview of the IoTSRM2 and describes the three-phased methodology for addressing the research questions of this study and in turn for determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2. Section 3 presents our IoTSRM2-based survey results. Then, Section 4 presents the related work. Finally, Section 5 presents the concluding remarks and future work.

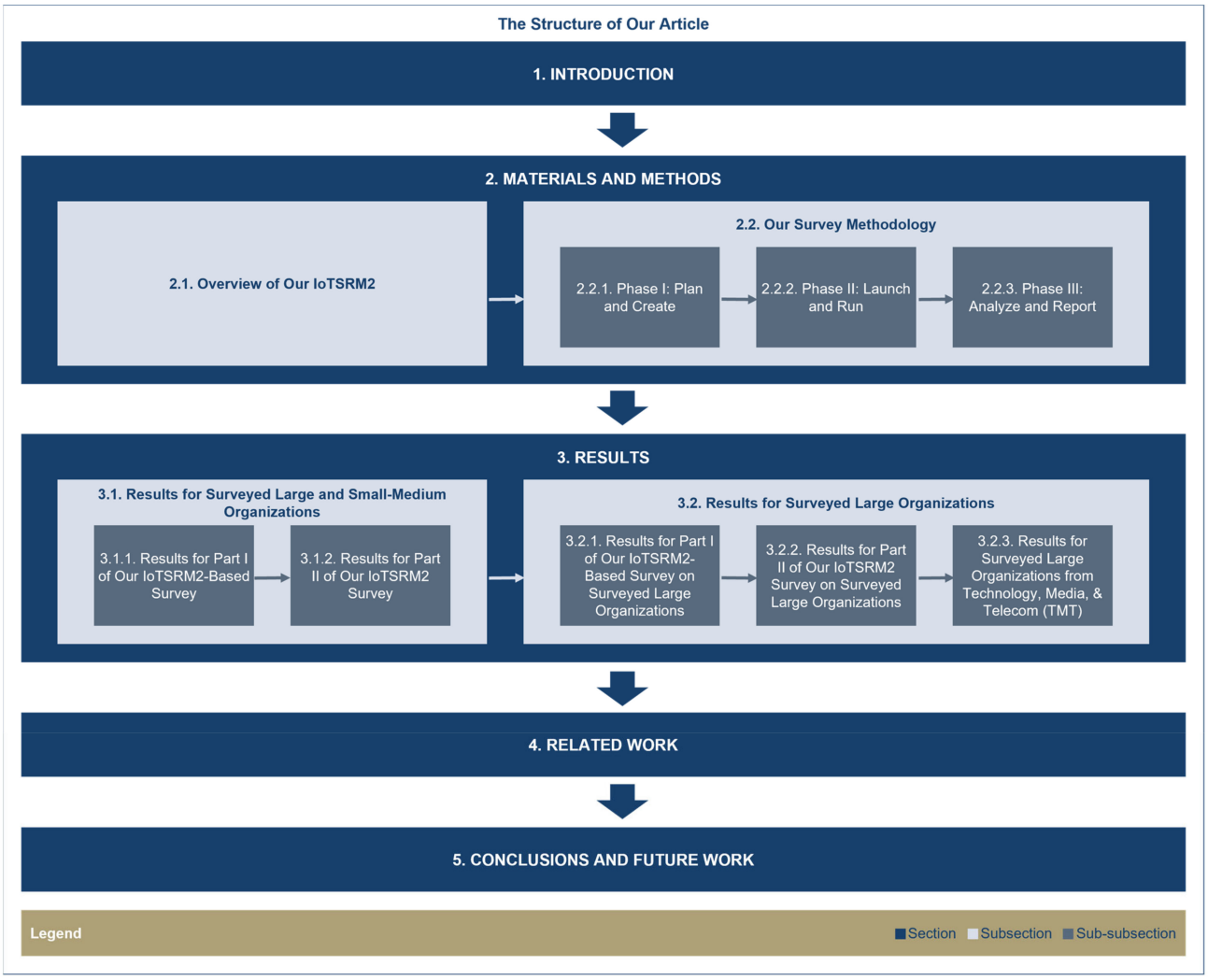

Figure 1. The structure of this article.

Then, Figure 2 provides a reading map for our research questions. This mapping should be leveraged in conjunction with the 14 research questions and Figure 1 by readers interested in specific research questions of our study, where:

- "Mapping 1" and "Mapping 2" correspond to the results sections related to the surveyed large and small-medium organizations;
- "Mapping 3", "Mapping 4", and "Mapping 5" correspond to the results sections related to the surveyed large organizations, where "Mapping 5" corresponds to the surveyed large organizations that operate in the "Technology, Media, & Telecom (TMT)" industry sector in particular.

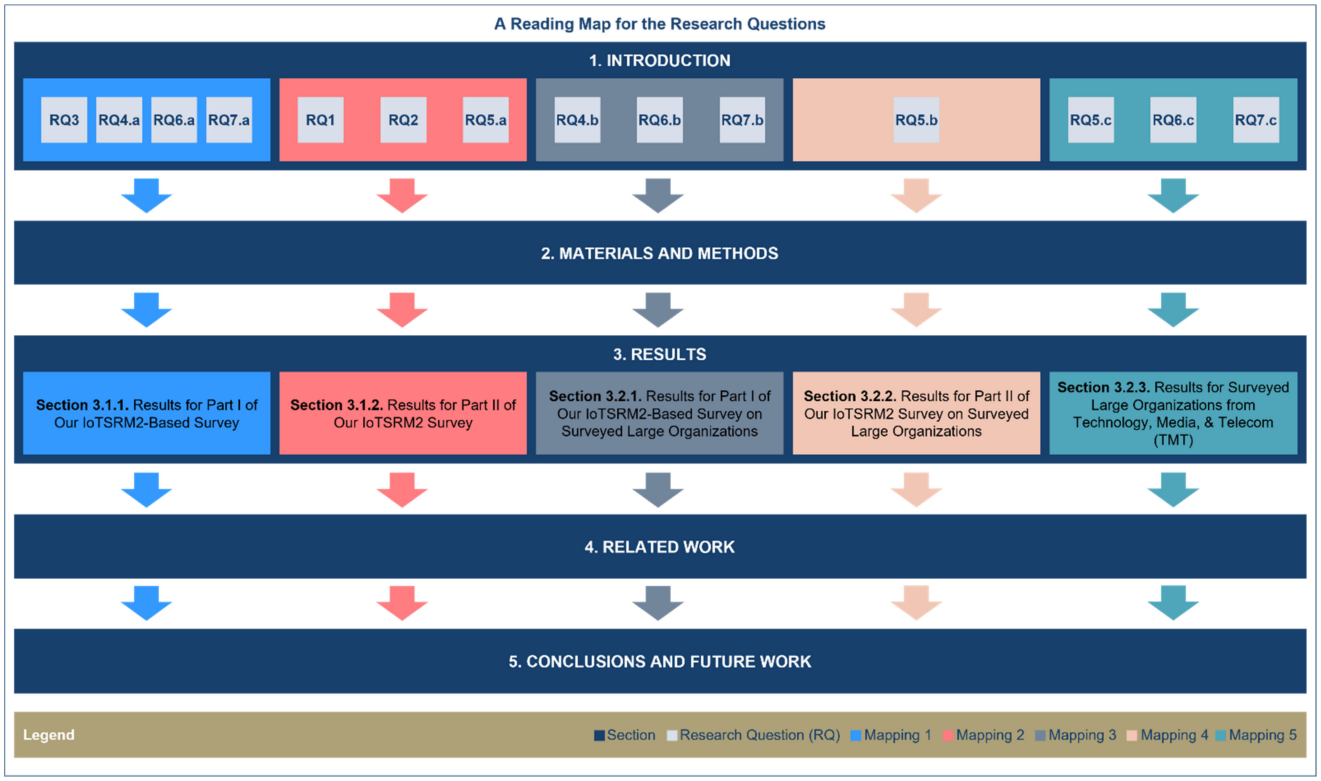

Figure 2. A reading map for our research questions.

For instance, assuming a reader is interested in RQ3, Figure 2 guides the reader via "Mapping 1" to read Sections 1, 2, 3.1.1, 4 and 5.

Furthermore, our mapping for possible items of interest from this article is provided in Appendix A as part of Table A1 which includes 25 selected items considered of interest and their corresponding sections, modes of presentation, main justification for inclusion, and indicative links.

2. Materials and Methods

This section is structured in two subsections. First, Section 2.1 provides an overview of our IoT Security Risk Management Strategy Reference Model (IoTSRM2). Then, Section 2.2 provides our survey methodology used for creating and running our IoTSRM2-based survey and for reporting our survey results on the current state of IoT security risk management strategies in the surveyed organizations relative to our IoTSRM2.

2.1. Overview of Our IoTSRM2

This subsection provides a summary of our IoT Security Risk Management Strategy Reference Model (IoTSRM2) which is applicable to IoT adopters from any sector, and which was proposed in our previous paper [14].

Figure 3 provides an illustrative overview of our IoTSRM2. Hence, this figure illustrates the 6 domains, 16 objectives, and 30 controls of IoTSRM2 for IoT adopters, which should be addressed by both IoT adopters and IoT suppliers [14]. Moreover, this figure indicates two IoTSRM2 controls that IoT adopters should review to establish whether these two are adequately implemented by IoT suppliers [14]. It is worth noting that each IoTSRM2 domain groups the corresponding IoTSRM2 objectives and each of these objectives groups the corresponding IoTSRM2 controls. These controls are based on 25 selected IoT security best practices and are described as part of our previous paper [14].

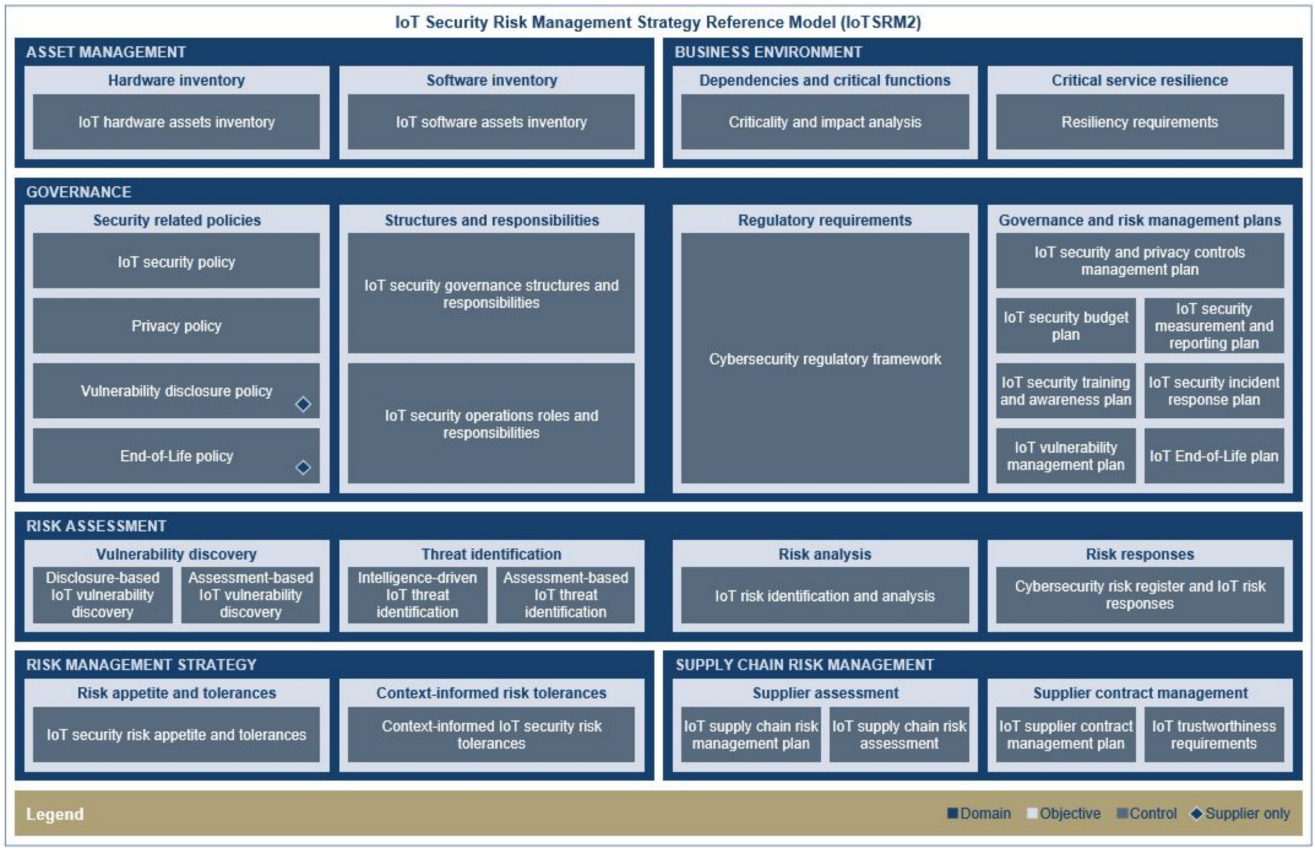

Figure 3. Our IoTSRM2 [14].

Furthermore, Table 1 shows the consolidated view of the IoTSRM2 controls, and it provides, for each of these controls, the unique identifier of and the corresponding adjusted control weight for that control [14]. It is worth noting that the adjusted control weights provide a means of prioritizing the IoTSRM2 controls for each IoTSRM2 objective [14].

Table 1. The IoTSRM2 controls with their adjusted weights [14].

Control ID	IoTSRM2 Control	Adjusted Control Weight
AM.A.1	IoT hardware assets inventory	6.25%
AM.B.1	IoT software assets inventory	6.25%
BE.A.1	Criticality and impact analysis	6.25%
BE.B.1	Resiliency requirements	6.25%
GV.A.1	IoT security policy	2.20%
GV.A.2	Privacy policy	1.67%
GV.A.3	Vulnerability disclosure policy	1.23%
GV.A.4	End-of-Life policy	1.15%
GV.B.1	IoT security governance structures and responsibilities	3.29%
GV.B.2	IoT security operations roles and responsibilities	2.96%
GV.C.1	Cybersecurity regulatory framework	6.25%
GV.D.1	IoT security and privacy controls management plan	2.14%
GV.D.2	IoT security budget plan	0.67%

Table 1. *Cont.*

Control ID	IoTSRM2 Control	Adjusted Control Weight
GV.D.3	IoT security measurement and reporting plan	0.35%
GV.D.4	IoT security training and awareness plan	0.96%
GV.D.5	IoT security incident response plan	0.62%
GV.D.6	IoT vulnerability management plan	0.89%
GV.D.7	IoT End-of-Life plan	0.63%
RA.A.1	Disclosure-based IoT vulnerability discovery	1.69%
RA.A.2	Assessment-based IoT vulnerability discovery	4.56%
RA.B.1	Intelligence-driven IoT threat identification	1.63%
RA.B.2	Assessment-based IoT threat identification	4.62%
RA.C.1	IoT risk identification and analysis	6.25%
RA.D.1	Cybersecurity risk register and IoT risk responses	6.25%
RM.A.1	IoT security risk appetite and tolerances	6.25%
RM.B.1	Context-informed IoT security risk tolerances	6.25%
SC.A.1	IoT supply chain risk management plan	3.90%
SC.A.2	IoT supply chain risk assessment	2.35%
SC.B.1	IoT supplier contract management plan	2.05%
SC.B.2	IoT trustworthiness requirements	4.20%

2.2. Our Survey Methodology

This subsection describes our methodology used for addressing the research questions of this study (see Section 1) and in turn for achieving the intended purpose of this research, namely determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoT Security Risk Management Strategy Reference Model (IoTSRM2). Figure 4 shows our proposed three-phased survey methodology that consists of nine steps and outputs, namely three steps with associated outputs for each of three phases (i.e., the plan and create, launch and run, and analyze and report phases).

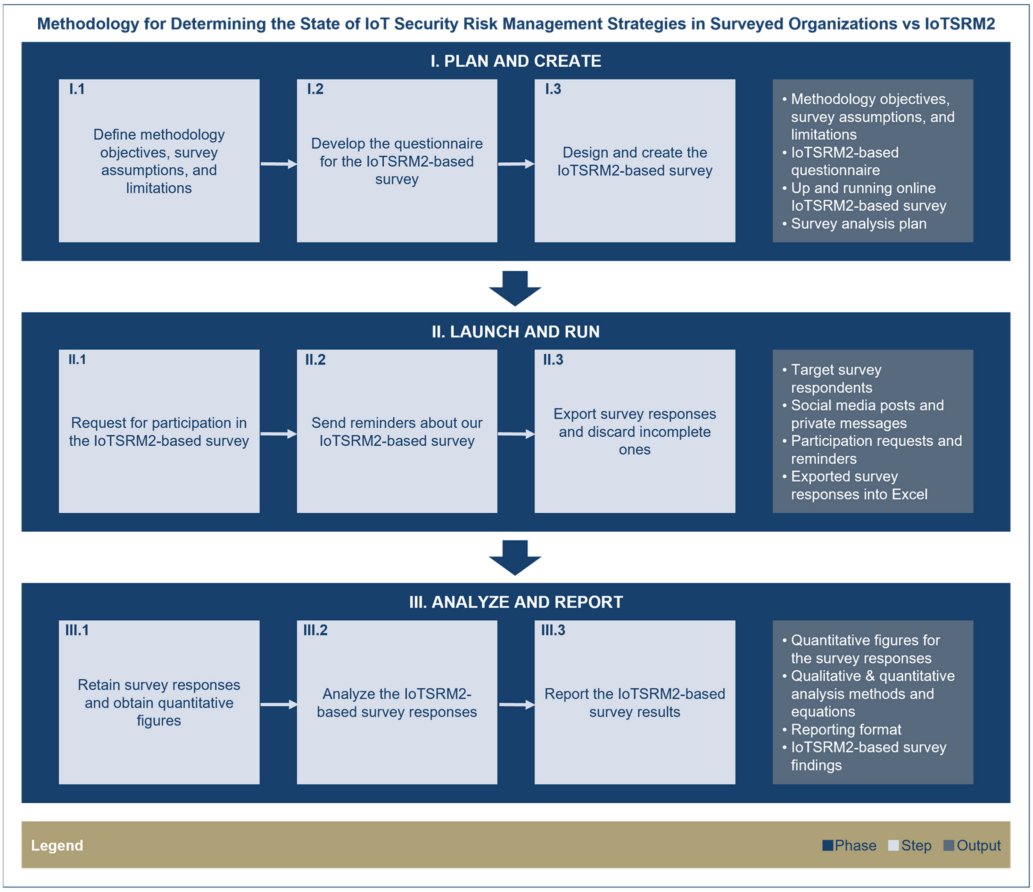

Figure 4. Our proposed three-phased survey methodology.

Furthermore, each of the three phases of our proposed methodology together with its corresponding steps are described below.

2.2.1. Phase I: Plan and Create

The "Plan and Create" phase involves the definition of methodology objectives, survey assumptions, and limitations (Step I.1), the development of the questionnaire for our IoTSRM2-based survey (Step I.2), and the design and creation of our IoTSRM2-based survey (Step I.3).

Step I.1: Define methodology objectives, survey assumptions, and limitations

First, this step outlines the twelve objectives of our proposed methodology. Thus, the main objective of the proposed methodology is:

- **Objective 1:** Run an online anonymous survey for four weeks based on the web survey design principles [20] and IoT Security Risk Management Strategy Reference Model (IoTSRM2) (see Section 2.1) targeting leaders with stake in IoT security risk management strategies from industries and governments from around the world to determine the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2.

Then, the secondary objectives of the proposed methodology are:

- **Objective 2:** Identify target groups of survey respondents to get the views of leaders from industries and governments on the IoT security risk management strategies of their organizations or client organizations relative to the IoTSRM2;
- **Objective 3:** Organize the questionnaire of our IoTSRM2-based survey in two parts, including screening and background questions for part I of and IoTSRM2-related questions for part II of our IoTSRM2-based survey;

- **Objective 4:** For part I of our IoTSRM2-based survey, formulate the screening and background questions with associated answer choices for each question to allow filtering and anonymous profiling of survey respondents and surveyed organizations;
- **Objective 5:** For part II of our IoTSRM2-based survey, formulate one IoTSRM2-related question with associated answer choices for each of the 30 IoTSRM2 controls (see Section 2.1) from our previous paper [14] to allow the determination of the current state of IoT security risk management strategies in the surveyed organizations based on IoTSRM2;
- **Objective 6:** Identify the principles for designing web questionnaires [20] that are applicable to our IoTSRM2-based survey to allow its corresponding design based on web survey design principles;
- **Objective 7:** Define the criteria for selecting an online survey tool that is fit for running our IoTSRM2-based survey;
- **Objective 8:** Develop the survey analysis plan for our IoTSRM2-based survey to focus the analysis of the survey responses on our research questions;
- **Objective 9:** Set up our IoTSRM2-based survey using the selected online survey tool to meet the applicable survey design principles and to include our questionnaire;
- **Objective 10:** Identify the target survey respondents that belong to the target groups of survey respondents and create social media posts and private messages that are aimed at increasing the survey response rate to request participation in our IoTSRM2-based survey;
- **Objective 11:** Send requests and reminders for survey participation through different distribution channels, including e-mail and social media (i.e., LinkedIn and Twitter);
- **Objective 12:** Analyze the collected survey responses based on our survey analysis plan and report our survey results for part I and II of our IoTSRM2-based survey for all surveyed organizations, the surveyed organizations of the top organization type by survey respondents, and the surveyed organizations from the top industry sector of the top organization type by survey respondents.

Furthermore, this step provides the assumptions on which our survey is based. These assumptions are split in two types: the underlying assumptions of the IoTSRM2 and the survey methodology assumptions. First, the underlying assumptions of the IoTSRM2 are listed below:

- "The cybersecurity risk management practices of IoT adopters prior to their IoT adoption and irrespective of their IoT security practices, are assumed to be agile and risk-informed, namely appraised at Tier 4 (Adaptive) of NIST CSF's Tiers [21]" [14];
- "IoT adopters are assumed to outsource IoT software development and not engage in in-house IoT software development activities" [14];
- "IoT adopters are assumed to have contracted IoT suppliers and conducted third-party IoT security due diligence reviews covering premarket IoT security related activities ahead of contracting IoT suppliers" [14].

Second, the assumptions on which the proposed survey methodology is based are listed below:

- Our survey respondents are assumed to provide genuine responses about the surveyed organizations;
- The underlying assumptions of the IoTSRM2 are assumed applicable for the surveyed organizations.

In addition, Step I.1 provides the limitations of our methodology and survey. These limitations are enumerated below:

- The proposed survey methodology is derived, based on, and limited to our professional judgement, IoT Security Risk Management Strategy Reference Model (IoTSRM2), and the selected survey design best practice;
- Our IoTSRM2-based survey is derived based on, and limited to, our survey methodology;

- Our IoTSRM2-based survey is limited to our survey methodology assumptions and the underlying assumptions of the IoTSRM2;
- Our IoTSRM2-based survey results are limited to the surveyed organizations and to the responses provided by our survey respondents. It is worth noting that any attempt to draw statistical inferences from our survey data about the current state of the IoT security risk management strategies in other organizations than the ones surveyed should be carefully navigated, is subject to survey biases (e.g., non-response bias, self-reporting bias), and is beyond the scope of this article.

Step I.2: Develop the questionnaire for the IoTSRM2-based survey

Step I.2 involves the development of the questionnaire for our IoTSRM2-based survey, which relies on the 30 IoTSRM2 controls (see Section 2.1) from our paper on the IoTSRM2 [14].

Thus, our questionnaire is divided into two parts. Part I includes five screening and background questions and part II includes 30 IoTSRM2-related questions. Both parts of our questionnaire contain only closed-ended questions.

With respect to part I of our IoTSRM2-based survey, Table 2 lists the screening and background questions of our questionnaire, and, for each question, it provides the associated possible answers and the justification of question inclusion. These screening and background questions are used to ensure the participation of the right survey respondents to our IoTSRM2-based survey and to allow categorization of the survey responses based on the anonymous profiles of the surveyed organizations. Hence, answering to these questions is a prerequisite for survey respondents to progress to the IoTSRM2-related questions of our IoTSRM2-based survey.

Table 2. Our screening and background questions with possible answers.

Question ID	Question	Possible Answers	Justification of Question Inclusion
Q1	To which organization are you referring when doing this survey?	My organization My client organization	The sole purpose of this background question is to enhance our collection of survey responses by targeting two types of survey respondents, namely either those from organizations that adopt IoT technologies or those from organizations that help their client organizations embrace IoT technologies.
Q2	Which of the following best describes your position?	C-level executive and/or board member Consulting practice leader and/or principal High-ranking government official Other senior position	This screening question aims to ensure the survey participation only of the organizational leaders that belong to the four target groups of survey respondents provided as possible answers for this question. It is worth noting that "Other senior position" refers to any other senior position of decision-making individuals.
Q3	What is the category of the organization?	Large Organization Small and Medium Sized Enterprise (SME)	For the purposes of this survey study, the organization type or the organization category is based on the size of the organization, and it can be either a small-medium organization or large organization. Hence, this background question aims to allow a clear delineation between the survey responses related to large organizations and those related to small-medium organizations. It is worth noting that SME denotes an organization having, inter alia, a staff headcount of less than 250 [22].
Q4	In which industry sector does the organization operate?	Education Energy & Utilities Financial & Insurance Services Government Healthcare Professional Services Technology, Media, & Telecom Other	This background question aims to allow a clear delineation between the survey responses related to the organizations that operate in different industry sectors.
Q5	In what region is the organization headquartered?	Asia Europe, Middle East and Africa (EMEA) North/South America Oceania	This background question aims to allow a clear delineation between the survey responses related to the organizations that are headquartered in different regions.

Then, with respect to part II of our IoTSRM2-based survey, Table 3 lists the 30 IoTSRM2-related questions of our IoTSRM2-based survey, and, for each IoTSRM2-related question, it provides the unique identifier of that question and the unique identifier of the corresponding IoTSRM2 control. Each of these IoTSRM2-related questions is formulated to cover one

of the 30 IoTSRM2 controls introduced in Section 2.1 of this paper and proposed in our previous paper on the IoTSRM2 [14]. Hence, these IoTSRM2-related questions are designed to get the leaders' views on the current state of the IoT security risk management control strategies of their organizations or client organizations against the IoTSRM2 controls.

Table 3. Our IoTSRM2-related questions.

Question ID	Question	IoTSRM2 Control ID
Q6	Does the organization have a comprehensive situational awareness on all its IoT hardware assets that leverages cybersecurity bills of materials (CBOMs) for all acquired IoT products and integration with its IT asset management processes?	AM.A.1
Q7	Does the organization have a comprehensive situational awareness on all its IoT software assets that leverages cybersecurity bills of materials (CBOMs) for all acquired IoT products and integration with its IT asset management processes?	AM.B.1
Q8	Does the organization prioritize all its IoT enabled services (e.g., customer services) and enablers (e.g., IoT components, IoT supply chain) based on their criticality to the organization, using cybersecurity bills of materials (CBOMs) for all acquired IoT products, and leveraging integration with cybersecurity risk management program?	BE.A.1
Q9	Does the organization keep, as part of its cybersecurity-related plans, up-to-date documented resiliency requirements (i.e., cybersecurity, reliability, continuity, and recovery) for all its mission critical IoT enabled services, and have high confidence in the cyber resilience of its IoT suppliers?	BE.B.1
Q10	Does the organization keep an up-to-date documented IoT security policy that is aligned with wider cybersecurity policy and formally approved, and contract only IoT suppliers that document and maintain robust cybersecurity policies incorporating IoT security considerations?	GV.A.1
Q11	Does the organization keep up-to-date documented IoT privacy requirements as part of its privacy policy that is aligned with wider data protection policy and formally approved, and receive privacy supplements from its IoT suppliers for all acquired IoT products and/or services?	GV.A.2
Q12	Do the organization's IoT suppliers keep up-to-date vulnerability disclosure policies that are clearly documented, publicly available, aligned with their vulnerability disclosure programs, and well communicated to all stakeholders?	GV.A.3
Q13	Do the organization's IoT suppliers keep up-to-date End-of-Life policies that are clearly documented, publicly available, aligned with their product and/or service lifecycle management strategies, and well communicated to all stakeholders?	GV.A.4
Q14	Does the organization keep up-to-date documented IoT security governance structures and responsibilities across and within the three lines of defense as part of its cybersecurity risk management program, and define shared governance structures and responsibilities for cybersecurity risk management with its IoT suppliers?	GV.B.1
Q15	Does the organization keep up-to-date documented IoT security operations roles and responsibilities as part of its cybersecurity risk management program, have dialogues on shared responsibility for IoT security with its IoT supplies, and maintain up-to-date points of contact for IoT security incident response and vulnerability disclosure from its IoT suppliers?	GV.B.2
Q16	Does the organization keep up-to-date documented IoT security and privacy requirements as part of its cybersecurity regulatory framework that is aligned with wider legal and regulatory framework, and work only with IoT suppliers that are aware of IoT security regulatory requirements and are transparent about their compliance with applicable legal and regulatory obligations?	GV.C.1
Q17	Does the organization keep an up-to-date documented IoT security and privacy controls management plan that is aligned with its cybersecurity risk management program and approved by board committees and/or C-suite executives, and contract only IoT suppliers that maintain robust cybersecurity-related controls frameworks incorporating IoT security requirements?	GV.D.1
Q18	Does the organization keep an up-to-date documented IoT security budget plan that is aligned with its cybersecurity budget plan and approved by board committees and/or C-suite executives, and contract only IoT suppliers that maintain up-to-date cybersecurity budget plans for secure IoT system development lifecycle?	GV.D.2

Table 3. *Cont.*

Question ID	Question	IoTSRM2 Control ID
Q19	Does the organization keep an up-to-date documented IoT security measurement and reporting plan that is aligned with its cybersecurity program measurement and reporting and formally approved, and have only IoT suppliers that maintain up-to-date IoT security measurement and reporting plans?	GV.D.3
Q20	Does the organization keep an up-to-date documented IoT security training and awareness plan that is aligned with its cybersecurity training and awareness program and formally approved, and have only IoT suppliers that maintain up-to-date IoT security training plans and share up-to-date user guides or manuals for all IoT products and/or services they provide?	GV.D.4
Q21	Does the organization keep an up-to-date documented IoT security incident response plan that is aligned with its cybersecurity incident response plan and formally approved, keep dialogues on shared responsibility for incident response with its IoT suppliers, and contract only IoT suppliers that maintain up-to-date cybersecurity incident response plans which incorporate IoT security considerations?	GV.D.5
Q22	Does the organization keep an up-to-date documented IoT vulnerability management plan that is aligned with its vulnerability management program and formally approved, and have only IoT suppliers that maintain robust vulnerability management and disclosure plans?	GV.D.6
Q23	Does the organization keep an up-to-date documented IoT End-of-Life plan that is aligned with its decommissioning strategy and formally approved, and contract only IoT suppliers that maintain robust End-of-Life policies and are transparent about their sunsetting plans?	GV.D.7
Q24	Does the organization continuously identify and document IoT vulnerabilities from multiple external sources as part of its cybersecurity risk assessment process, and have only IoT suppliers that incentivize third-party vulnerability reporting and release timely security advisories for the IoT products and/or services they provide?	RA.A.1
Q25	Does the organization continuously or periodically identify and document IoT vulnerabilities using a blend of various assessment processes as part of its cybersecurity risk assessment process, and work only with IoT suppliers that engage in continuous or periodic cybersecurity assessments to achieve ongoing vulnerability monitoring and cybersecurity improvement?	RA.A.2
Q26	Does the organization continuously identify and document IoT threats from multiple external threat sharing sources as part of its cybersecurity risk assessment process, and work only with IoT suppliers that engage in cyber threat information sharing and leverage effective vulnerability disclosure programs to identify cyber threats to the IoT products and/or services they provide?	RA.B.1
Q27	Does the organization continuously or periodically identify and document IoT threats using a blend of conventional and cyber kill chain based assessments as part of its cybersecurity risk assessment process, and work only with IoT suppliers that engage in cybersecurity assessments to maintain a robust situational awareness on the cyber threats relevant for the IoT products and/or services they provide?	RA.B.2
Q28	Does the organization regularly identify and analyze IoT security and privacy risks as part of its cybersecurity risk assessment process, and work only with IoT suppliers that continuously monitor and assess the risks of confidentiality, integrity, availability, and safety of the IoT products and/or services they provide being compromised?	RA.C.1
Q29	Does the organization have a comprehensive situational awareness on its IoT security and privacy risks that leverages an up-to-date documented cybersecurity risk register which is aligned with the enterprise cybersecurity risk register, and have high confidence in the cybersecurity risk management capabilities of its IoT suppliers?	RA.D.1
Q30	Does the organization clearly articulate and document IoT security risk appetite and tolerances in line with its appetites and tolerances for cybersecurity and privacy risks, and contract only IoT suppliers that are transparent about their appetites and associated tolerances for cybersecurity, privacy, and IoT security risks?	RM.A.1
Q31	Does the organization have a comprehensive situational awareness around its role in critical infrastructure and sector risk profile that informs its IoT security risk tolerance statement, and have high confidence that the IoT risk tolerances of its IoT suppliers are context-informed?	RM.B.1

Table 3. *Cont.*

Question ID	Question	IoTSRM2 Control ID
Q32	Does the organization keep an up-to-date documented IoT supply chain risk management plan that is aligned with its broader cyber supply chain risk management program and formally approved, and contract only IoT suppliers that maintain robust cyber supply chain risk management plans covering their whole IoT supply chains?	SC.A.1
Q33	Does the organization regularly assess and record IoT supply chain risks across its supply chain tiers based on its IoT supply chain risk management plan, and work only with IoT suppliers that continuously or regularly assess their cybersecurity and privacy supply chain risks and are transparent about their findings?	SC.A.2
Q34	Does the organization keep an up-to-date documented IoT supplier contract management plan that is aligned with its broader cyber supply chain risk management program and formally approved, and work only with IoT suppliers that maintain robust supplier contract management plans and are transparent about relevant supply chain changes?	SC.B.1
Q35	Does the organization keep, as part of its IoT supplier contract management plan, up-to-date documented IoT trustworthiness requirements (i.e., cybersecurity, privacy, safety, reliability, and resiliency) for its IoT supplier contracts, and contract only IoT suppliers that deliver up-to-date cybersecurity bills of materials (CBOMs) for the IoT products they provide and have IoT supplier contracts that enable IoT supply chain of trust?	SC.B.2

Furthermore, Table 4 outlines the selected answer format for the 30 IoTSRM2-related questions. This table lists four possible answers, and it gives, for each possible answer, the description of each answer choice and the corresponding percentage score that provides a means to quantitatively rate that answer choice for quantitative analysis of survey responses. Hence, the answer format of our IoTSRM2-related questions is a four-point Likert scale with the answer choices "No, to a great extent", "No, to a certain extent", "Yes, to a certain extent", and "Yes, to a great extent", where the middle point is deliberately excluded to avoid indecisive answers [23]. Moreover, these possible answers are designed for survey respondents to rate the extent to which their organizations or client organizations meet each of the IoTSRM2-related questions by selecting one of these answer choices for each of these questions.

Table 4. The answer format of our IoTSRM2-related questions.

Possible Answer	Description	Percentage Score
No, to a great extent	The organization's current control deviates from the expected IoTSRM2 control with major discrepancies.	0%
No, to a certain extent	The organization's current control nearly deviates from the expected IoTSRM2 control with some similarities. This current control state varies across surveyed organizations having a tendency towards deviating from the "as-is" IoTSRM2 control, which may average around 25% and considers an additional tolerance of 5% to avoid downgrading the associated percentage score too much.	30%
Yes, to a certain extent	The organization's current control fairly meets the expected IoTSRM2 control with minor discrepancies. This current control state varies across surveyed organizations having a tendency towards meeting the "as-is" IoTSRM2 control, which may average around 75% and considers a negative tolerance of 5% to avoid favoring the associated percentage score too much.	70%
Yes, to a great extent	The organization's current control fully meets the expected IoTSRM2 control with no apparent discrepancies.	100%

Step I.3: Design and create the IoTSRM2-based survey

Step I.3 involves the design of our survey based on the principles for designing web questionnaires developed by Dillman et al. [20] and on the structure and content of our questionnaire (see Step I.2). Thus, Table 5 lists these principles for designing web questionnaires, and, for each of these principles, it indicates whether it is applicable to our IoTSRM2-based survey, and it provides our justification of the applicability of that principle.

Table 5. The applicability of the principles for designing web questionnaires to our IoTSRM2-based survey.

No.	Principle	Applicability	Justification of Applicability
1.	"Introduce the web questionnaire with a welcome screen that is motivational, emphasizes the ease of responding, and instructs respondents on the action needed for proceeding to the next page." [20]	Applicable	Our IoTSRM2-based survey is designed to have a welcome screen. This welcome screen shows the name of our survey, a thank you message to all our survey participants for taking the time to participate in our survey, the purpose of our survey, the assumptions on which the IoTSRM2 is based, along with the structure of our survey. A screenshot of the welcome screen of our IoTSRM2-based survey is provided in Appendix B as part of Figure A1.
2.	"Begin the web questionnaire with a question that is fully visible on the first screen of the questionnaire, and will be easily comprehended and answered by all respondents." [20]	Applicable	Following the welcome screen, our IoTSRM2-based survey is designed to begin with a single question that asks our survey respondents to select the organization to which they are referring to when undertaking our survey. A screenshot with our first question from our IoTSRM2-based survey is provided in Appendix B as part of Figure A2.
3.	"Present each question in a conventional format similar to that normally used on paper questionnaires." [20]	Applicable	Our IoTSRM2-based survey is designed to have each question associated with a unique identifier and to have all possible answers for any given question listed vertically underneath that question.
4.	"Limit line length to decrease the likelihood of a long line of prose being allowed to extend across the screen of the respondent's browser." [20]	Applicable	Our IoTSRM2-based survey is structured in two parts: the screening and background questions and the IoTSRM2-related questions (see Step I.2). While the screening and background questions are short, the IoTSRM2-related questions are formulated to cover the entire content of the IoTSRM2 controls, which may increase their length. Notwithstanding, our IoTSRM2-based survey aims to leverage a survey platform that allows this principle being met.
5.	"Provide specific instructions on how to take each necessary computer action for responding to the questionnaire." [20]	Applicable	The welcome screen of our IoTSRM2-based survey is designed to provide sufficient details around the assumptions on which the IoTSRM2 is based and around the structure of our survey. This allows our survey respondents to have visibility on the underlying assumptions of our IoTSRM2 and over the two categories of questions being asked throughout our survey (i.e., the screening and background questions and the IoTSRM2-related questions). In addition, following the first question of the screening and background part, our IoTSRM2-based survey is designed to include a note at the beginning of each page of the questionnaire which is aimed to remind our survey respondents throughout our questionnaire what the word "organization" denotes (i.e., their organization or client organization depending on their answer to the first question of our IoTSRM2-based survey).

Table 5. *Cont.*

No.	Principle	Applicability	Justification of Applicability
6.	"Provide computer operation instructions as part of each question where the action is to be taken, not in a separate section prior to the beginning of the questionnaire." [20]	Applicable	Our IoTSRM2-based survey is designed to notify our survey respondents, through an error message, about any unanswered questions from any given page before being allowed to move to the next page. In addition, our questionnaire targets only computer literate respondents and is designed to include only closed-ended questions. Thus, there is no other need for computer operation instructions or specific response instructions.
7.	"Do not require respondents to provide an answer to each question before being allowed to answer any subsequent ones." [20]	Applicable	Our IoTSRM2-based survey is designed to allow our survey respondents to respond to questions in any order within any page of our survey.
8.	"Construct web questionnaires so that they scroll from question to question unless order effects are a major concern, large numbers of questions must be skipped, and/or a mixed-mode survey is being done for which telephone interview and web results will be combined." [20]	Applicable	Our multipage IoTSRM2-based survey is designed to allow our survey respondents to scroll from question to question within any page of our survey, and the navigation from one page to another is conditioned by the completion of all actions from that page. Moreover, following the first question of the screening and background part, our IoTSRM2-based survey is designed to include a note at the beginning of each page of the questionnaire which reminds our survey respondents what the word "organization" denotes (i.e., their organization or client organization) and encourages them to review their response to question 1 if necessary.
9.	"When the number of answer choices exceeds the number that can be displayed on one screen, consider double-banking with appropriate navigational instructions being added." [20]	Not applicable	Our IoTSRM2-based survey is designed to display all answer choices on the screen in a visible manner for all questions.
10.	"Use graphical symbols or words that convey a sense of where the respondent is in the completion progress, but avoid ones that require advanced programming." [20]	Applicable	Our IoTSRM2-based survey is designed to have a progress bar that allow respondents to have visibility on their completion progress. The progress bar can be observed in the screenshot provided in Appendix B as part of Figure A1.
11.	"Be cautious about using question structures that have known measurement problems on paper questionnaires, e.g., check-all-that-apply and open-ended questions." [20]	Applicable	Our IoTSRM2-based survey is designed to include only closed-ended questions that are measurable (see Step I.2).

Furthermore, Step I.3 provides our criteria defined for the selection of the online survey tool which is used to set up and run our IoTSRM2-based survey. Thus, Table 6 provides these selection criteria, and it outlines, for each selection criterion, the corresponding justification of inclusion for the selection of the online survey tool.

Table 6. Our criteria for selecting the online survey tool.

No.	Selection Criterion	Justification of Inclusion
1.	The online survey tool provides features that allow the creation of our online IoTSRM2-based survey following the principles for designing web questionnaires developed by Dillman et al. [20].	The online survey tool of choice should allow the creation of our online IoTSRM2-based survey based on the web survey design principles developed by Dillman et al. [20], which will make way for a better survey experience for our respondents and a higher response rate.
2.	The online survey tool allows for anonymous responses.	The online survey tool should keep the data of our respondents anonymous to encourage our survey respondents to share their views without being worried of breaching confidentiality and non-disclosure agreements. This may boost the response rate and improve the quality of survey responses.
3.	The online survey tool allows the inclusion of the 35 questions of our questionnaire.	The online survey tool should accommodate the inclusion of our 35-items questionnaire to allow the collection of survey responses to the screening and background questions and to the 30 IoTSRM2-related questions.
4.	The online survey tool provides the feature that allows the creation of mobile friendly surveys.	The online survey tool should have the mobile friendly feature given that our IoTSRM2-based survey is targeting leaders and seniors who are frequently using mobile devices, and our intention is that our IoTSRM2-based survey to be available for both desktop and mobile devices.
5.	The online survey tool provides the feature that allows the export of the survey responses in the Excel file format.	The online survey tool should provide the ability of exporting the survey responses in the Excel file format. This is because the analysis of the survey responses will use the Excel software.
6.	The online survey tool is a well renowned online survey tool.	Running our IoTSRM2-based survey using a widely used online survey tool may increase the likelihood that the target survey respondents respond to our survey.

Thus, considering the six selection criteria outlined above, the SurveyMonkey tool is selected for the creation of our IoTSRM2-based survey. Moreover, the setup of our IoTSRM2-based survey is guided by the principles for designing web questionnaires developed by Dillman et al. [20], uses the Momentive's guidance for creating a survey [24], follows the structure of our questionnaire (see Step I.2), and includes the content of our questionnaire (see Step I.2). In addition, this setup activity involves the testing of our IoTSRM2-based survey prior to having it up and running.

Furthermore, Step I.3 involves the development of our survey analysis plan to ensure that the outputs of our methodology help in addressing our research questions. Irwin and Stafford [25] endorsed this approach to ensure that the development of the survey is on track with the intended survey outcomes.

Thus, Table 7 outlines our survey analysis plan which maps the survey questions (i.e., "IoTSRM2-Based Survey Question IDs"), the intended analysis method (i.e., "Potential Analysis Method"), and the intended presentation of the results (i.e., "Potential Presentation of Results) to each of the research questions and its corresponding unique identifier.

Table 7. Our proposed survey analysis plan.

Research Question ID	Research Question	IoTSRM2-Based Survey Question IDs	Potential Analysis Method	Potential Presentation of Results
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?	Q6–Q35	For each IoTSRM2 control and related question: % of survey responses of ("Yes, to a certain extent" and "Yes, to a great extent") compared with % of survey responses of ("No, to a great extent" and "No, to a certain extent")	Figure showing, for each IoTSRM2 control and related question, the overall tendency of the survey responses towards either deviating from or meeting that IoTSRM2 control.
RQ2	What is the IoTSRM2 compliance score of each of the surveyed organizations?	Q6–Q35	For each surveyed organization: IoTSRM2 compliance score	Column chart showing, for each surveyed organization, the IoTSRM2 compliance score, corresponding region, and whether this score is less than 50% or greater or equal to 50%.
RQ3	Which is the top organization type for the surveyed organizations by survey respondents?	Q3	% distribution of the survey responses by organization type	Pie chart showing the % distribution of the responses to our IoTSRM2-based survey by organization type for the surveyed organizations.
RQ4.a	Which is the top industry sector for the surveyed organizations by survey respondents?	Q4	% distribution of the survey responses by industry sector for the surveyed organizations	Pie chart showing the % distribution of the responses by industry sector for the surveyed organizations.
RQ4.b	Which is the top industry sector for the surveyed organizations of the top organization type by survey respondents?	Q3–Q4	% distribution of the survey responses by industry sector for the surveyed organizations of the top organization type	Pie chart showing the % distribution of the responses by industry sector for the surveyed organizations of the top organization type.
RQ5.a	What is the overall average IoTSRM2 compliance score of the surveyed organizations for each IoTSRM2 control?	Q6–Q35	For each IoTSRM2 control and related question: overall average compliance score of surveyed organizations with IoTSRM2 controls	Figure showing, for each IoTSRM2 control and related question, the overall average IoTSRM2 compliance score of the surveyed organizations and whether this score is less than 50% or greater or equal to 50%.

Table 7. *Cont.*

Research Question ID	Research Question	IoTSRM2-Based Survey Question IDs	Potential Analysis Method	Potential Presentation of Results
RQ5.b	What is the overall average IoTSRM2 compliance score of the surveyed organizations of the top organization type for each IoTSRM2 control?	Q6–Q35	For each IoTSRM2 control and related question: overall average compliance score of surveyed organizations of the top organization type with IoTSRM2 controls	Figure showing, for each IoTSRM2 control and related question, the overall average IoTSRM2 compliance score of the surveyed organizations of the top organization type and whether this score is less than 50% or greater or equal to 50%.
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?	Q6–Q35	For each IoTSRM2 control and related question: Overall average compliance score of surveyed organizations from the top industry sector of the top organization type with IoTSRM2 controls	Figure showing, for each IoTSRM2 control and related question, the overall average IoTSRM2 compliance score of the surveyed organizations from the top industry sector of the top organization type and whether this score is less than 50% or greater or equal to 50%.
RQ6.a	Which is the top position level of the survey respondents for the surveyed organizations by survey respondents?	Q2	% distribution of the survey respondents by position level for the surveyed organizations	Pie chart showing the % distribution of the survey respondents by position level for the surveyed organizations.
RQ6.b	Which is the top position level of the survey respondents for the surveyed organizations of the top organization type by survey respondents?	Q2–Q3	% distribution of the survey respondents by position level for the surveyed organizations of the top organization type	Pie chart showing the % distribution of the survey respondents by position level for the surveyed organizations of the top organization type.
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?	Q2–Q4	% distribution of the survey respondents by position level for the surveyed organizations from the top industry sector of the top organization type	Pie chart showing the % distribution of the survey respondents by position level for the surveyed organizations from the top industry sector of the top organization type.
RQ7.a	Which is the top region for the surveyed organizations by survey respondents?	Q5	% distribution of the survey responses by region for the surveyed organizations	Pie chart showing the % distribution of the survey responses by region for the surveyed organizations.

Table 7. *Cont.*

Research Question ID	Research Question	IoTSRM2-Based Survey Question IDs	Potential Analysis Method	Potential Presentation of Results
RQ7.b	Which is the top region for the surveyed organizations of the top organization type by survey respondents?	Q3, Q5	% distribution of the survey responses by region for the surveyed organizations of the top organization type	Pie chart showing the % distribution of the survey responses by region for the surveyed organizations of the top organization type.
RQ7.c	Which is the top region for the surveyed organizations from the top industry sector of the top organization type by survey respondents?	Q3–Q5	% distribution of the survey responses by region for the surveyed organizations from the top industry sector of the top organization type	Pie chart showing the % distribution of the survey responses by region for the surveyed organizations from the top industry sector of the top organization type.

2.2.2. Phase II: Launch and Run

The "Launch and Run" phase involves the request for participation in our IoTSRM2-based survey (Step II.1), the submission of reminders about our IoTSRM2-based survey (Step II.2), and the export of survey responses to Excel and the rejection of incomplete survey responses (Step II.3).

Step II.1: Request for participation in the IoTSRM2-based survey

Step II.1 involves the identification of target survey respondents for our sampling frame, and the request for participation of the target respondents in our IoTSRM2-based survey. First, the identification of the target survey respondents is based on our target groups of survey respondents selected in Step I.2. Second, the request for participation in our IoTSRM2-based survey entails the creation of social media posts and private messages for requesting participation in our IoTSRM2-based survey, and the delivery of these messages using the distribution channels decided on in Step I.1.

Furthermore, our social media posts and private messages for requesting participation in our survey are designed to increase the response rate of our survey by employing several widely used techniques. First, our private messages leverage personalization for engaging with each of our target survey respondents as described by Frippiat and Marquis [26]. Moreover, our social media posts and private messages apply three of the survey responses theories (i.e., exchange theory, self-perception theory, and commitment and involvement) studied by Keusch [27]. These theories were also employed in the study conducted by Poon et al. [28] to invite or induce participation as part of a laboratory-type experiment. Thus, besides providing key details on our IoTSRM2-based survey (e.g., the access link to our survey), our social media posts, and private messages feature a combination of the following techniques:

- **Personalization:** the private messages are personalized for engaging with each of our target survey respondents by starting the message with an informal greeting (e.g., "Hello John");
- **Exchange theory:** the private messages ask our target survey respondents to complete our survey and/or share it to the right individuals from their teams for getting access to our survey results once these get published (i.e., "Once our next article is published, you will be able to benchmark your organization or client organization against peers");
- **Self-perception theory:** the self-perception theory is applied as part of our social media posts by asking prestigious IoT-engaged leaders to complete our survey and/or share it to the right individuals from their teams, which labels them as being IoT

engaged (i.e., "we are please asking prestigious IoT-engaged leaders to share their views and or share our survey with the right people");

- **Commitment/involvement:** our social media posts and private messages clearly articulate the importance of our IoTSRM2-based survey topic (e.g., "IoTSRM2 relies on 25 IoT security best practices and is the result of an extensive research work") and of participating in our IoTSRM2-based survey by getting the chance to have their opinions heard (i.e., "Our survey seeks views from leaders from industries and governments on the IoT security risk management strategies of their organizations or client organizations").

Step II.2: Send reminders about our IoTSRM2-based survey

Step II.2 involves sending a combination of reminders including private messages and social media posts about our IoTSRM2-based survey. This activity of using a blend of reminders aims to reduce the number of individual reminders being sent and to increase the survey response rate. According to the studies conducted by Keusch [27] and Sánchez-Fernández et al. [29], sending a reduced number of reminders is considered to have a positive influence on survey response rates.

Step II.3: Export survey responses and discard incomplete ones

Step II.3 involves the export of all survey responses from SurveyMonkey to Excel once our survey ends. At this point, all individual survey responses that are incomplete are discarded to ensure only clean survey responses are retained for the analysis and reporting.

2.2.3. Phase III: Analyze and Report

The "Analyze and Report" phase involves obtaining quantitative figures for the survey responses on top of the original survey responses (Step III.1), the qualitative and quantitative analysis of the IoTSRM2-based survey responses (Step III.2), and the reporting of our IoTSRM2-based survey results (Step III.3).

Step III.1: Retain survey responses and obtain quantitative figures

Step III.1 involves retaining the exported survey responses in their original form and converting a copy of the qualitative IoTSRM2-related responses into quantitative figures as outlined in the study conducted by Combs and Onwuegbuzie [30]. This translation of survey responses into quantitative figures leverages the percentage scores corresponding to the possible answers of the IoTSRM2-related questions (see Step I.2).

Hence, for each survey respondent, the quantitative figures (i.e., the percentage scores) are represented using Equation (1), where Q_j represents the 30 IoTSRM2-related questions (i.e., from Q6 to Q35), Response_i (Q_j) represents the responses of the survey respondents to the IoTSRM2-related questions, 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:

$$\begin{gathered} \text{Convert } (\text{Response}_i(Q_j)) = R_{ij}, \\ \text{where } R_{ij} = \begin{cases} 0, \ \text{Response}_i(Q_j) = \text{“No, to a great extent”} \\ 30\%, \ \text{Response}_i(Q_j) = \text{“No, to a certain extent”} \\ 70\%, \ \text{Response}_i(Q_j) = \text{“Yes, to a certain extent”} \\ 100\%, \ \text{Response}_i(Q_j) = \text{“Yes, to a great extent”} \end{cases} \\ i = [1..K], \ j = [6..35], \text{ and } K = |\text{survey respondents}| \end{gathered} \tag{1}$$

Step III.2: Analyze the IoTSRM2-based survey responses

This step involves the analysis of all survey responses across three groups of surveyed organizations. First, the analysis is performed across all surveyed organizations. Second, the analysis focuses on the surveyed organizations of top organization type by survey respondents. Finally, the analysis is conducted on the surveyed organizations from the top industry sector of the top organization type by survey respondents.

Thus, Figure 5 shows the overview of our intended analysis of the survey responses for part I and II of our IoTSRM2-based survey across three groups of surveyed organizations.

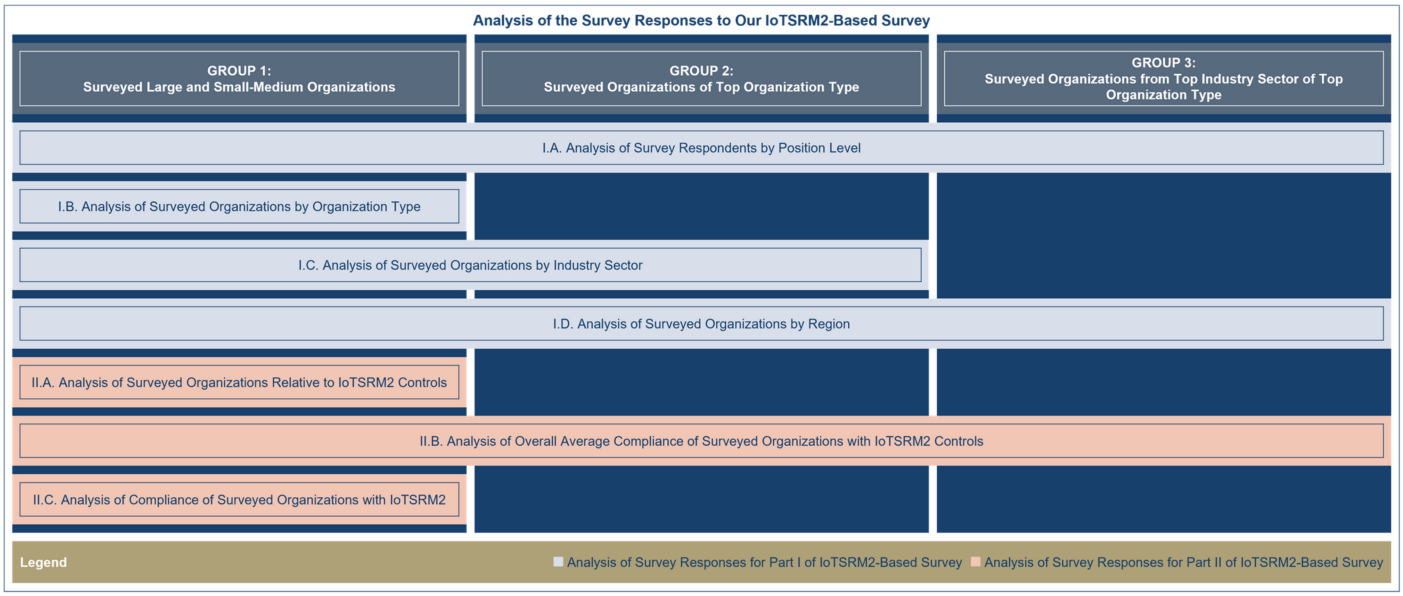

Figure 5. Outline of our analysis of the responses to our IoTSRM2-based survey.

Thus, with respect to the analysis of the survey responses for part I of the IoTSRM2-based survey, first, the analysis of survey respondents by position level (i.e., I.A) is intended across all three groups of surveyed organizations (i.e., the surveyed large and small-medium organizations, the surveyed organizations of the top organization type, and the surveyed organizations from the top industry sector of the top organization type). This analysis (i.e., I.A) aims to address the RQ6.a, RQ6.b, and RQ6.c research questions (see Step I.3), and it involves exploring the percentage distribution of the survey respondents by position level for each group of survey respondents. Second, the analysis of the surveyed organizations by organization type (i.e., I.B) is intended for the first group of surveyed organizations. This analysis (i.e., I.B) aims to address the RQ3 research question (see Step I.3), and it involves exploring the percentage distribution of the surveyed organizations by organization type for the surveyed large and small-medium organizations. Third, the analysis of the surveyed organizations by industry sector (i.e., I.C) is intended for the first two groups of surveyed organizations. This analysis (i.e., I.C) aims to address the RQ4.a and RQ4.b research questions (see Step I.3), and it involves exploring the percentage distribution of the surveyed organizations by industry sector for the surveyed large and small-medium organizations and for the surveyed organizations of top organization type. Finally, the analysis of the surveyed organizations by region (i.e., I.D) is intended to span all three groups of surveyed organizations. This analysis (i.e., I.D) aims to address the RQ7.a, RQ7.b, and RQ7.c research questions (see Step I.3), and it involves exploring the percentage distribution of the surveyed organizations by region for all three groups of surveyed organizations.

Then, with respect to the analysis of the survey responses for part II of the IoTSRM2-based survey, first, the analysis of the surveyed organizations relative to the IoTSRM2 controls (i.e., II.A) is intended for the first group of surveyed organizations. This analysis (i.e., II.A) aims to address the RQ1 research question (see Step I.3), and it involves examining the survey responses in their qualitative form by comparing, for each IoTSRM2-related question, 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".

Second, the analysis of the overall average compliance of the surveyed organizations with the IoTSRM2 controls (i.e., II.B) is intended for all three groups of surveyed organizations. This analysis (i.e., II.B) aims to address the RQ5a, RQ5.b, and RQ5.c research questions (see Step I.3), and it involves computing, for each IoTSRM2 control and related

question for each of the three groups of surveyed organizations, the overall average compliance score based on the quantitative figures for the survey responses and the corresponding adjusted control weight.

Hence, first, for each survey respondent and for each IoTSRM2 control and related question, this analysis (i.e., II.B) feeds the quantitative figures that result from using Equation (1) (see Step III.1) together with the corresponding adjusted control weight (see Section 2.1) into Equation (2) to determine the compliance of the corresponding surveyed organization with that IoTSRM2 control and related question. Note that in Equation (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 (see Table 1 from Section 2.1 and Table 3 from Section 2.2.1), R_{ij} represents the percentage scores corresponding to survey respondents for the IoTSRM2-related questions (see Step III.1), Adjusted weight (C_j) represents the adjusted weights corresponding to the IoTSRM2 controls (see Table 1 from Section 2.1), and K represents the cardinality of the survey respondents.

$$\begin{gathered}\text{Compliance}_i(C_j) = R_{ij} \times \text{Adjusted weight } (C_j) \\ \text{where } i = [1..K],\ j = [6..35],\ \text{and } K = |\text{survey respondents}|\end{gathered} \tag{2}$$

Second, after computing the compliance score with each of the IoTSRM2 controls for each of the surveyed organizations, this analysis (i.e., II.B) is intended for each of the three groups of surveyed organizations and aims to determine, for each IoTSRM2 control and related question, the overall average compliance score and whether this score shows a tendency towards deviating from (i.e., less than 50%) or meeting (i.e., greater than or equal to 50%) the "as-is" IoTSRM2 control. These overall average compliance scores are represented using Equation (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), $\text{Compliance}_i(C_j)$ represents the compliance scores of the surveyed organizations with the IoTSRM2 controls, and C_j represents the IoTSRM2 controls that correspond to the IoTSRM2-related questions (see Table 1 from Section 2.1 and Table 3 from Section 2.2.1).

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

Finally, the analysis of the compliance of the surveyed organizations with IoTSRM2 (i.e., II.C) is intended for the first group of surveyed organizations. This analysis (i.e., II.C) aims to address the RQ2 research question (see Step I.3), and it involves determining, for each of the surveyed organizations, the IoTSRM2 compliance score using Equation (4). In this equation, $\text{IoTSRM2 compliance score}_i$ represents the IoTSRM2 compliance scores of the surveyed organizations, $\text{Compliance}_i(C_j)$ 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 (see Table 1 from Section 2.1 and Table 3 from Section 2.2.1), and K represents the cardinality of the survey respondents.

$$\begin{gathered}\text{IoTSRM2 compliance score}_i = \sum_{j=6}^{35} \text{Compliance}_i(C_j), \\ \text{where } i = [1..K],\ j = [6..35],\ K = |\text{survey respondents}|\end{gathered} \tag{4}$$

Moreover, to allow for the anonymous nature of and enable an easier analysis and understanding of the survey responses, this analysis (i.e., II.C) leverages our proposed naming convention for identifying each of the surveyed organizations, where name parts are separated by dots. These name parts are outlined below:

- The organization category identifier, which shows the type of the organization in question, specifically "LG" for large organizations or "SM" for small-medium organizations;
- The industry classification identifier, which shows the industry sector of the organization in question, specifically "EDU" for "Education", "E&U" for "Energy & Utilities", "FSO" for "Financial & Insurance Services", "GOV" for "Government", "HSO" for "Healthcare", "PSO" for "Professional Services", "TMT" for "Technology, Media, & Telecom", or "OTH" for "Other";
- The sequence number of the organization within the group of surveyed organizations of the same organization category and industry sector.

For instance, LG.TMT.1 denotes the first surveyed large organization from the "Technology, Media, & Telecom (TMT)" industry sector, while the SM.TMT.1 denotes the first surveyed small medium organization from the "Technology, Media, & Telecom (TMT)" industry sector.

Step III.3: Report the IoTSRM2-based survey results

This step involves the reporting of our IoTSRM2-based survey results for each of the three groups of surveyed organizations outlined in Step III.2, namely:

- **Group 1:** the surveyed large and small-medium organizations;
- **Group 2:** the surveyed organizations of the top organization type;
- **Group 3:** the surveyed organizations from the top industry sector of the top organization type.

Furthermore, Figure 6 provides the intended structure for reporting our IoTSRM2-based survey findings.

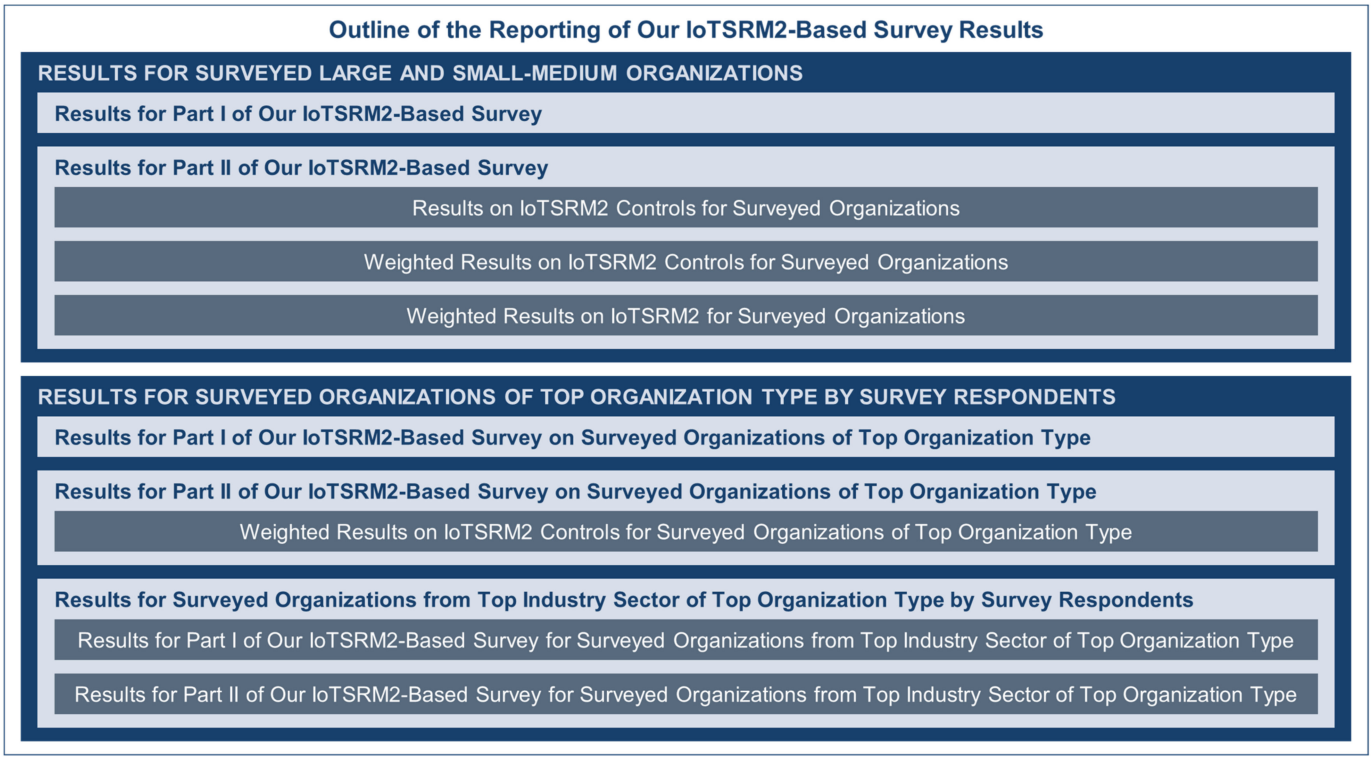

Figure 6. Outline of our reporting for the IoTSRM2-based survey results.

Hence, with respect to the Group 1 of surveyed organizations, the reporting involves:

- Providing the survey results derived from the analysis (i.e., I.A, I.B, I.C, I.D) of the survey responses for part I of the IoTSRM2-based survey (see Step III.2);

- Providing the survey results derived from the analysis (i.e., II.A, II.B, II.C) of the survey responses for part II of the IoTSRM2-based survey (see Step III.2).

Then, with respect to the Group 2 of surveyed organizations, the reporting involves:

- Providing the survey results derived from the analysis (i.e., I.A, I.C, I.D) of the survey responses for part I of the IoTSRM2-based survey (see Step III.2);
- Providing the survey results derived from the analysis (i.e., II.B) of the survey responses for part II of the IoTSRM2-based survey (see Step III.2).

Finally, with respect to the Group 3 of surveyed organizations, the reporting involves:

- Providing the survey results derived from the analysis (i.e., I.A, I.D) of the survey responses for part I of the IoTSRM2-based survey (see Step III.2);
- Providing the survey results derived from the analysis (i.e., II.B) of the survey responses for part II of the IoTSRM2-based survey (see Step III.2).

3. Results

This section presents our IoTSRM2-based survey results and is structured in two subsections as depicted in Figure 7. Section 3.1 focuses on our survey results for the surveyed large and small-medium organizations. First, Section 3.1.1 provides the results for part I of our IoTSRM2-based survey. Second, Section 3.1.2 provides the results for part II of our IoTSRM2-based survey by focusing on the IoTSRM2 controls and on the entire IoTSRM2 for the surveyed organizations. Subsequently, Section 3.2 focuses exclusively on our survey results for the surveyed organizations of the top organization type by survey respondents (see Section 2.2), namely on the surveyed large organizations. First, Section 3.2.1 provides the results for part I of our IoTSRM2-based survey on the surveyed large organizations. Second, Section 3.2.2 provides the results for part II of our IoTSRM2-based survey on the surveyed large organizations by focusing on the corresponding IoTSRM2 controls. Third, Section 3.2.3 narrows the focus on the surveyed large organizations from the top industry sector by survey respondents (see Section 2.2), namely on the surveyed large organizations from the Technology, Media, and Telecom (TMT) industry sector, and provides the results for part I and II of our IoTSRM2-based survey on the surveyed large TMT organizations.

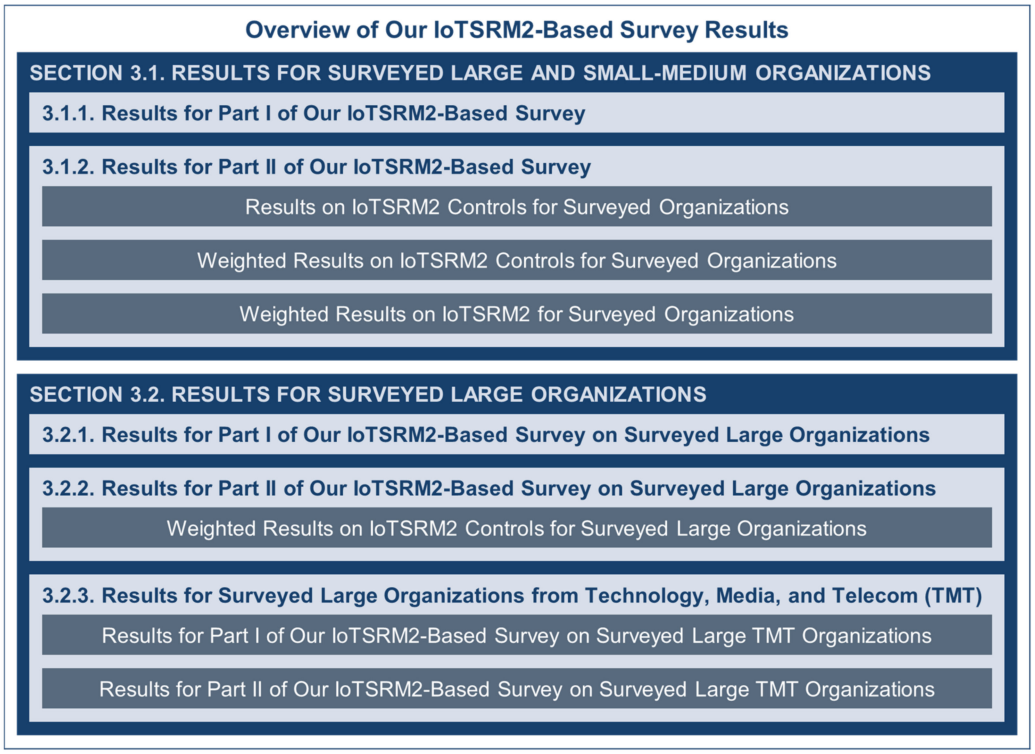

Figure 7. Outline of the structure of our IoTSRM2-based survey results.

3.1. Results for Surveyed Large and Small-Medium Organizations

This subsection is structured in two subsubsections. First it provides the results for part I of our IoTSRM2-based survey, and then it provides the results for part II of our IoTSRM2-based survey.

Following our IoTSRM2-based survey, which was conducted between 14 June and 12 July 2021, Table 8 shows the key details on the responses to our IoTSRM2-based survey including the sampling frame of 1502 leaders and seniors with stake in cybersecurity and/or technology risk management strategies, the number of collected individual survey responses (i.e., the survey returns), the number of discarded surveys (see Step II.3 of the "Launch and Run" phase of our survey methodology from Section 2.2.2), the final sample of 31 leaders and seniors with stake in IoT security risk management strategies, and the survey response rate of 2.1%.

Table 8. Key details on the responses to our IoTSRM2-based survey.

Sampling Frame	Survey Returns	Discarded Surveys	Final Sample	Survey Response Rate
1502 [1]	63	32	31	2.1%

[1] Note that this figure includes only target survey respondents that were sent private messages for survey participation request.

3.1.1. Results for Part I of Our IoTSRM2-Based Survey

This subsubsection provides our main results for part I of our IoTSRM2-based survey including the percentage distribution of our survey respondents by position level, and the percentage distributions of the responses to our IoTSRM2-based survey by organization category, industry sector, and region.

Thus, Figure 8 shows the percentage distribution of the survey respondents by position level, which reveals that the majority of our survey respondents (i.e., 84%) correspond to and are evenly distributed across the "C-level executive and/or board member" and "Consulting practice leader and/or principal" position levels. Hence, these two position

levels of our survey respondents resulted in having the top percentage score for the surveyed organizations by survey respondents.

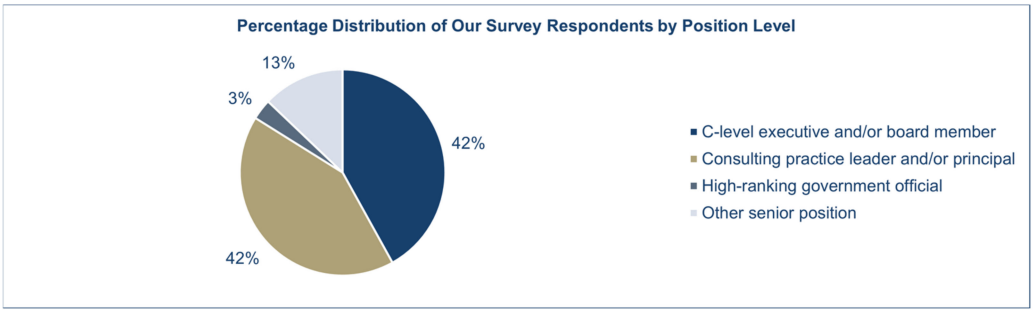

Figure 8. Distribution of our survey respondents by position level.

Furthermore, Figure 9 shows the percentage distribution of the responses to our IoTSRM2-based survey by organization type (i.e., based on the organization size). In other words, this figure shows the percentage distribution of our survey respondents' organizations of focus for this survey by organization category. Hence, it reveals that the "Large Organization" category makes up the greater part of the survey respondents' organizations of focus for this survey (i.e., the surveyed organizations), which makes the "Large Organization" category the top organization type by survey respondents for our IoTSRM2-based survey. It is worth noting that these organizations of focus may indicate the organizations or client organizations of our survey respondents depending on what they were referring to when completing our IoTSRM2-based survey.

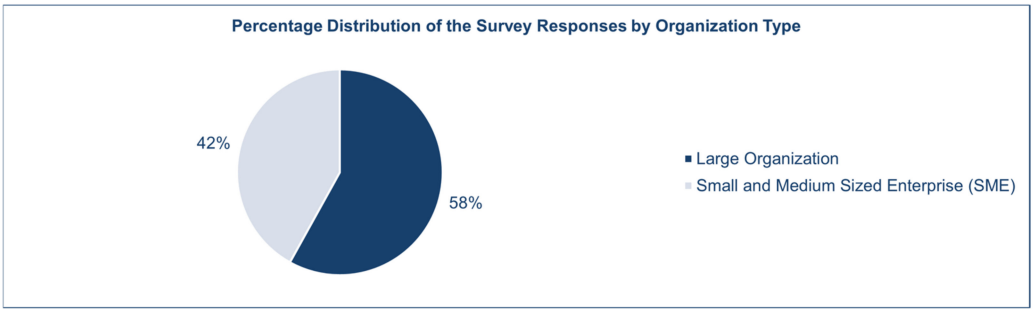

Figure 9. Distribution of survey responses by organization category.

Then, Figure 10 presents the percentage distribution of the responses to our IoTSRM2-based survey by industry classification. In other words, this figure shows the percentage distribution of our survey respondents' organizations or client organizations by industry sector. Hence, it reveals that the "Technology, Media, & Telecom (TMT)" industry sector makes up the top industry sector for our survey respondents' organizations of focus for this survey (i.e., the surveyed organizations).

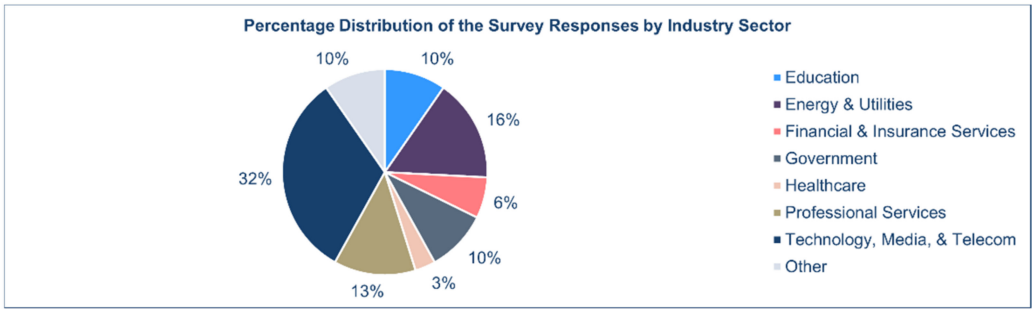

Figure 10. Distribution of survey responses by industry classification.

Then, Figure 11 shows the percentage distribution of the organizations of focus of our survey respondents for this survey by region, which reveals that the majority of the responses to our IoTSRM2-based survey (i.e., around 81%) correspond to organizations headquartered in the "Europe, Middle East and Africa (EMEA)" and "North/South America" regions. Moreover, it is worth noting that the "North/South America" region resulted in having the top percentage score for the surveyed organizations by survey respondents.

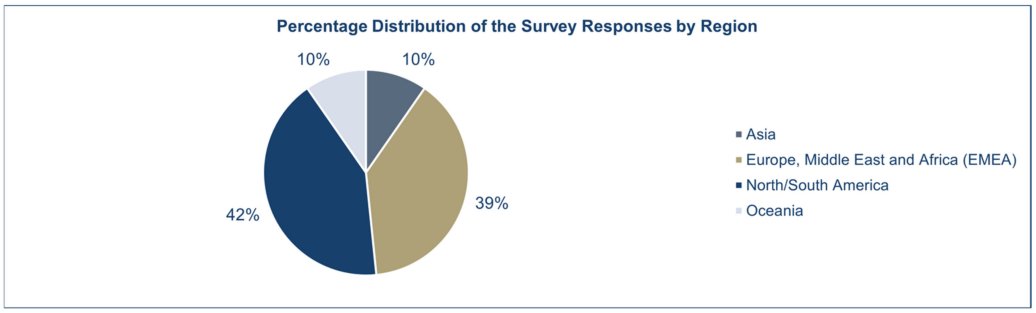

Figure 11. Distribution of our survey responses by region.

3.1.2. Results for Part II of Our IoTSRM2 Survey

This subsubsection provides our main results for part II of our IoTSRM2-based survey, including the results on the IoTSRM2 controls along with the weighted results on the IoTSRM2 controls and on the entire IoTSRM2 for the surveyed organizations.

Results on IoTSRM2 Controls for Surveyed Organizations

First, Section 3.1.2 outlines the key results on the IoTSRM2 controls for the survey respondents' organizations or client organizations (i.e., the surveyed organizations) by showing the IoTSRM2 view for the survey responses to our IoTSRM2-related questions.

Thus, Figure 12 provides the IoTSRM2 view for the survey responses to our IoTSRM2-related questions and highlights for each IoTSRM2 control and related question the overall tendency of the corresponding survey responses (i.e., towards either deviating from or meeting the "as-is" IoTSRM2 control in question). This figure aims to allow readers to rapidly pinpoint, for each IoTSRM2 control and related question, how the majority of our survey respondents answered, specifically it enables readers to picture, for each IoTSRM2 control and related question, the concentrations of survey responses across two groups of answer choices (i.e., "Yes, to a certain and great extent" and "No, to a certain and great extent"). A consolidated view of the summary of the survey responses in numbers for each IoTSRM2-related question and IoTSRM2 control is provided in Appendix C as part of Table A2 which includes the number of survey responses corresponding to each answer choice for the IoTSRM2-related questions.

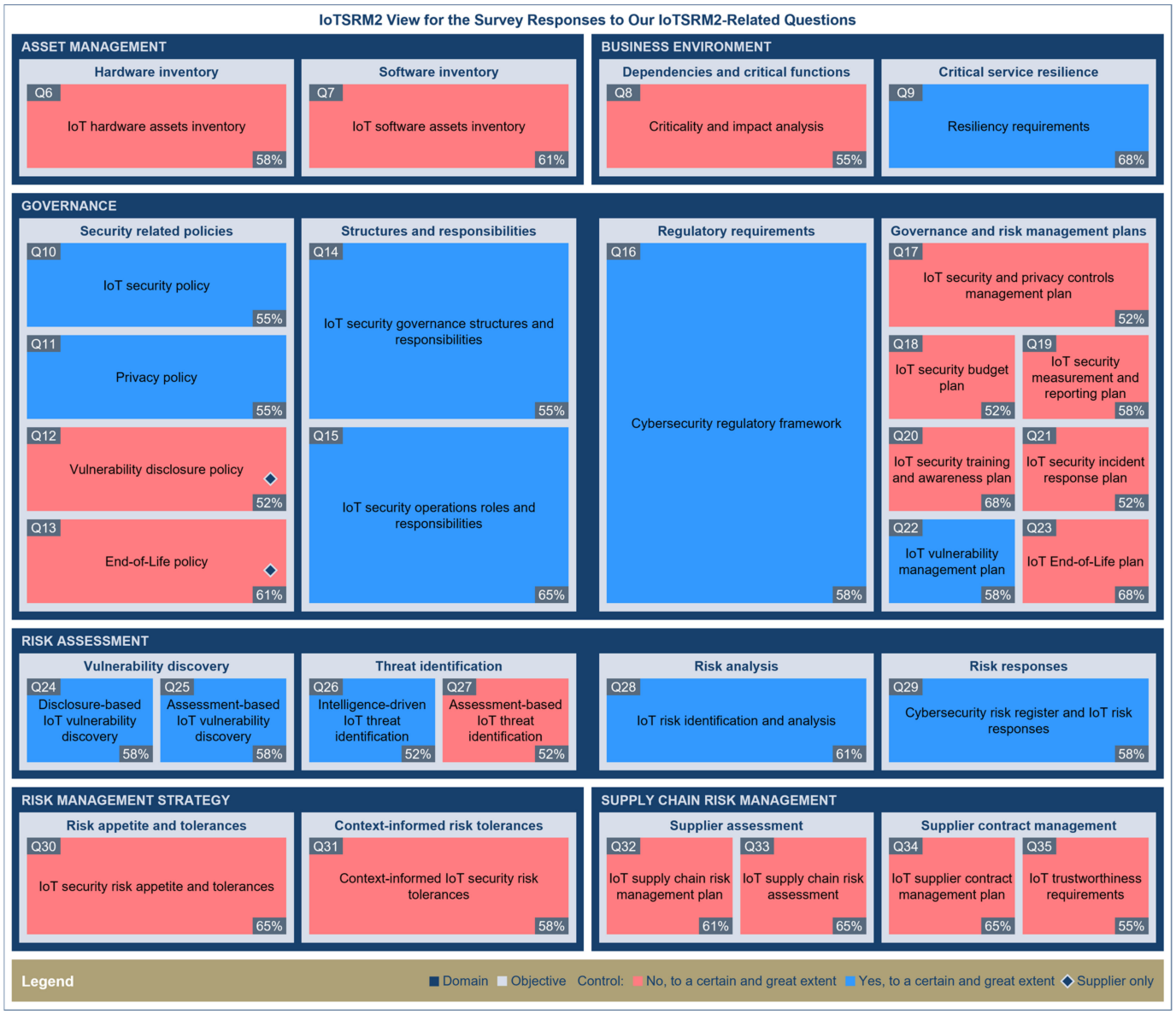

Figure 12. IoTSRM2 overview for the responses to our IoTSRM2-based survey. Adapted from [14].

First, with respect to the "Yes, to a certain and great extent" group of answer choices from Figure 12, this group corresponds to and highlights each IoTSRM2 control and related question for which the percentage of survey responses of "Yes, to a certain extent" and "Yes, to a great extent" of the total number of survey responses for that IoTSRM2-related question exceeds the percentage of survey responses of "No, to a great extent" and "No, to a certain extent" of the total number of survey responses for that IoTSRM2-related question. Hence, Figure 12 shows that the majority of survey respondents answered either "Yes, to a certain extent" or "Yes, to a great extent" to the following IoTSRM2-related questions (i.e., the question IDs in descending order by percentage of survey responses): Q9, Q15, Q28, Q16, Q22, Q24, Q25, Q29, Q10, Q11, Q14, and Q26.

Then, about the "No, to a certain and great extent" group of answer choices, this group corresponds to and highlights each IoTSRM2 control and related question for which the percentage of survey responses of "No, to a great extent" and "No, to a certain extent" of the total number of survey responses for that IoTSRM2-related question exceeds the percentage of survey responses of "Yes, to a certain extent" and "Yes, to a great extent" of the total number of survey responses for that IoTSRM2-related question. Hence, Figure 12

shows that the majority of survey respondents answered either "No, to a great extent" or "No, to a certain extent" to the following IoTSRM2-related questions (i.e., the question IDs in descending order by percentage of survey responses): Q20, Q23, Q34, Q33, Q30, Q32, Q13, Q7, Q31, Q19, Q6, Q35, Q8, Q27, Q21, Q18, Q17, and Q12.

Therefore, considering where the heavy concentrations of the survey responses are across the two groups of answer choices for each IoTSRM2 control and related question, the majority of the surveyed organizations resulted in having the highest performance in the "Risk Assessment" and "Business Environment" domains, in that order, whereas the majority of the surveyed organizations resulted in having the lowest performance in the "Asset Management", "Risk Management Strategy", "Supply Chain Risk Management", and "Governance" domains, in that order.

First, with respect to the "Risk Assessment" domain, except for the "Assessment-based IoT threat identification" control, the majority of the survey responses are "Yes, to a certain extent" and "Yes, to a great extent" for the corresponding IoTSRM2 controls (i.e., "Disclosure-based IoT vulnerability discovery", "Assessment-based IoT vulnerability discovery", "Intelligence-driven IoT threat identification", "IoT risk identification and analysis", and "Cybersecurity risk register and IoT risk responses") and related questions. This result shows that, although most of the surveyed organizations are not so preoccupied with undertaking comprehensive IoT threat profiling exercises, these organizations do engage in IoT risk assessments.

Second, about the "Business Environment" domain, while most of the survey responses are "No, to a great extent" and "No, to a certain extent" for the "Criticality and impact analysis" control and related question, most of the survey responses for the "Resiliency requirements" control and related question are "Yes, to a certain extent" and "Yes, to a great extent". On the one hand, our finding suggests that most of the surveyed organizations are not so preoccupied with prioritizing IoT related assets based on their criticality to the organization, which may indicate that most surveyed organizations adopt one-size-fits-all approaches in defending IoT enabled services and enablers. On the other hand, our finding shows that the majority of the surveyed organizations are very preoccupied with improving the resilience of their IoT infrastructures, which may suggest that most surveyed organizations focus on securing their IoT infrastructure resilience to compensate for their intake of IoT security and privacy risks.

Then, with respect to the "Asset Management" domain, the majority of survey responses are "No, to a great extent" and "No, to a certain extent" for both corresponding IoTSRM2 controls (i.e., "IoT hardware assets inventory" and "IoT software assets inventory") and related questions. This result shows that most of the surveyed organizations lack all-encompassing IoT asset inventories, which may exacerbate shadow IoT in these organizations and diversify the unknown attack vectors for these organizations.

Afterwards, with respect to the "Risk Management Strategy" domain, the majority of survey responses are "No, to a great extent" and "No, to a certain extent" for both corresponding IoTSRM2 controls (i.e., "IoT security risk appetite and tolerances" and "Context-informed IoT security risk tolerances") and related questions. This finding suggests that most surveyed organizations adopt either one-size-fits-all or ad hoc approaches in managing their IoT security and privacy risks which may drive deep disproportionalities or inefficiencies and inconsistencies in the execution of their IoT security risk management strategies, respectively.

Subsequently, with respect to the "Supply Chain Risk Management" domain, the majority of survey responses are "No, to a great extent" and "No, to a certain extent" for all four corresponding IoTSRM2 controls (i.e., "IoT supply chain risk management plan", "IoT supply chain risk assessment", "IoT supplier contract management plan", and "IoT trustworthiness requirements") and related questions. This finding reveals that most surveyed organizations underperform when it comes to managing IoT supply chain risk which may increase the likelihood of IoT supply chain risk occurrence given that IoT adoption amplifies the interdependencies between the surveyed organizations and

their supply chains. This is because they tend to manage their relationships with their IoT suppliers in an ad hoc fashion rather than relying on structured IoT supply chain risk assessments and trustworthiness requirements underpinned by clearly defined IoT supply chain risk management and IoT supplier contract management plans.

As for the "Governance" domain, the majority of the survey responses are "Yes, to a certain extent" and "Yes, to a great extent" for the "IoT security policy", "Privacy policy", "IoT security operations roles and responsibilities", "IoT security governance structures and responsibilities", "Cybersecurity regulatory framework", and "IoT vulnerability management plan" controls and related questions, whereas the majority of the survey responses are "No, to a great extent" and "No, to a certain extent" for the "Vulnerability disclosure policy", "End-of-Life policy", "IoT security and privacy controls management plan", "IoT security budget plan", "IoT security measurement and reporting plan", "IoT security training and awareness plan", "IoT security incident response plan", and "IoT End-of-Life plan" controls and related questions. This finding suggests that although most surveyed organizations have IoT security and privacy policies, understand their compliance obligations, and have IoT security governance structures and responsibilities in place, they underperform in strategizing governance and risk management for their IoT infrastructures (i.e., except for vulnerability management) and fail in ensuring that their IoT suppliers have clearly documented vulnerability disclosure and End-of-Life policies in place. Hence, considering that the majority of the surveyed organizations may rely on a relatively fragile base for crafting their IoT security risk management strategy, this finding is quite worrying for these organizations as it may have cascading consequences on the execution of their IoT security risk management strategy.

In this context, the majority of the surveyed organizations should consider reviewing and improving their controls related to the IoTSRM2 controls of the "Asset Management", "Risk Management Strategy", "Supply Chain Risk Management", and "Governance" domains.

Weighted Results on IoTSRM2 Controls for Surveyed Organizations

Second, Section 3.1.2 outlines the key results on the IoTSRM2 controls for the surveyed organizations by outlining the overall average compliance with IoTSRM2 controls. The overall average IoTSRM2 compliance score for each IoTSRM2 control and related question resulted based on all survey responses and the corresponding IoTSRM2 adjusted control weight for that IoTSRM2 control and related question. It is worth noting that, for each IoTSRM2 control, the overall average IoTSRM2 compliance score is calculated using Equations (1)–(3) (see Section 2.2.3).

Furthermore, Figure 13 presents the consolidated view of the survey responses through the corresponding overall average IoTSRM2 compliance score for each IoTSRM2 control and related question. For each IoTSRM2 control and related question, this figure indicates whether the corresponding overall average IoTSRM2 compliance score leans towards deviating from or meeting the "as-is" IoTRSM2 control.

Figure 13 shows that the overall average IoTSRM2 compliance score across the survey respondents' organizations or client organizations (i.e., the surveyed organizations) is less than 50% for the majority of the IoTSRM2 controls and only marginally greater than 50% for the remaining eleven IoTSRM2 controls. Thus, the "Resiliency requirements", "IoT security operations roles and responsibilities", and "IoT risk identification and analysis" controls resulted in having the top three highest overall average IoTSRM2 compliance scores, in that order, whereas the "IoT security training and awareness plan", "IoT supplier contract management plan", "IoT End-of-Life plan", "IoT software assets inventory", and "IoT supply chain risk assessment" controls resulted in having the top three lowest overall average IoTSRM2 compliance scores, in that order.

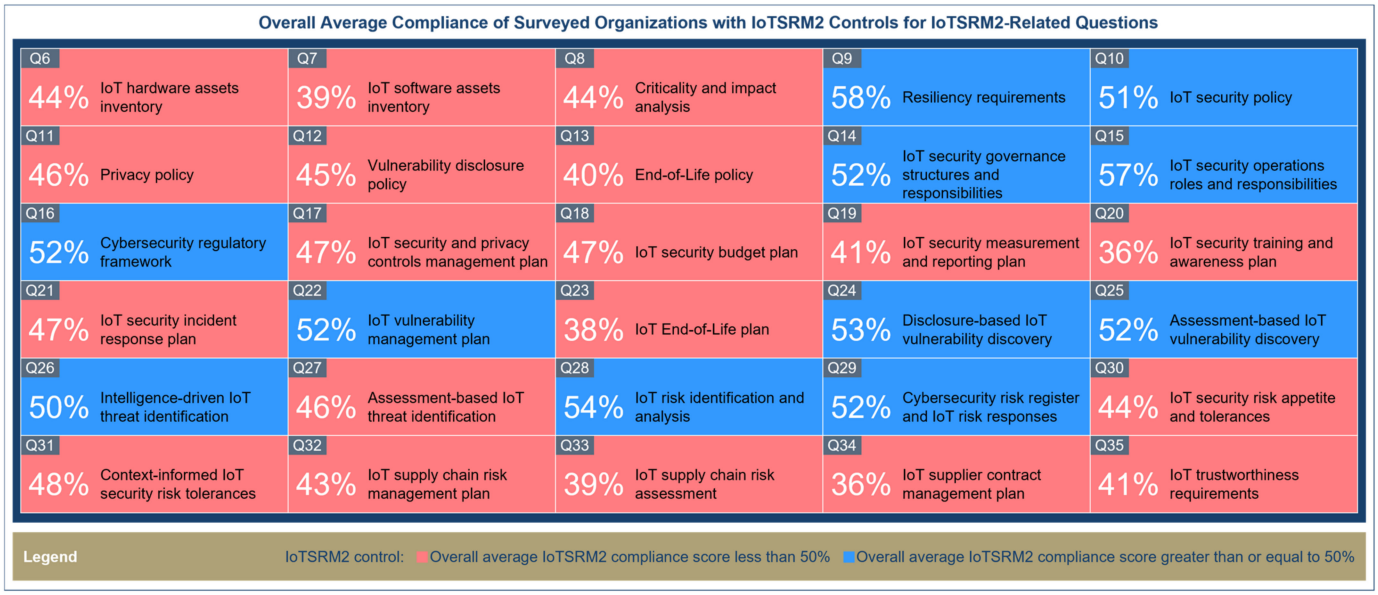

Figure 13. Overall average compliance with IoTSRM2 controls based on the survey responses.

First, with respect to the top three highest overall average IoTSRM2 compliance scores, these findings suggest that the majority of the surveyed organizations (i.e., the survey respondents' organizations or client organizations of focus for our IoTSRM2-based survey) concentrate on building security operations and resilience capabilities to withstand and recover rapidly from imminent cyber-attacks, and they adopt a more proactive approach to address IoT security and privacy risks by leveraging IoT security risk assessments.

Second, with regard to the "IoT security training and awareness plan" control, our survey result shows that the majority of the surveyed organizations lack the "as-is" IoTSRM2 control on the IoT security training and awareness. This finding of our survey suggests that most surveyed organizations are not well informed on or do not clearly understand the IoT security and privacy risks they face, which may lead them to being more susceptible to poor formulation and/or execution of IoT security risk management strategies, which may in turn lead to unsecure IoT technology adoption, usage of unsecure IoT technologies, and propagation of cyber-attacks due to not knowing whether their IoT infrastructure is breached or where and how to rapidly report suspicious/unusual IoT activity.

Then, with respect to the "IoT supplier contract management plan" control, our survey finding reveals that the majority of the surveyed organizations deviate or nearly deviate from the "as-is" corresponding IoTSRM2 control. This result of our survey shows that most surveyed organizations may be exposed to heightened levels of IoT supply chain risk due to engaging in ad hoc rather than well planned IoT supply chain risk management practices that might omit dealing with certain IoT supply chain risks and in effect fail to provide an adequate level of defense against nefarious or security negligent third party entities.

With respect to the "IoT End-of-Life plan" control, our survey result reveals that the majority of the surveyed organizations deviate or nearly deviate from the "as-is" corresponding IoTSRM2 control. This result of our survey suggests that most surveyed organizations are likely to end up using outdated and unsupported IoT technologies and having difficulties in adequately hardening their IoT technologies which would substantially increase their IoT attack surface in the long run.

Then, about the "IoT software assets inventory" control, our survey result reveals that the majority of the surveyed organizations deviate or nearly deviate from the "as-is" corresponding IoTSRM2 control. This finding of our survey suggests that most surveyed organizations may already experience different extents of shadow IoT software, which for some of them may be way beyond their IoT security risk appetites without knowing it.

As for the "IoT supply chain risk assessment" control, our survey result shows that the majority of the surveyed organizations deviate or nearly deviate from the "as-is" corresponding IoTSRM2 control. This finding of our survey suggests that most surveyed organizations do not actively assess their IoT supply chain risks across several supply chain tiers, which may not only hinder their ability to adequately enforce a base level of trust across their supply chain but also diminish their ability to rapidly identify and mitigate the IoT security-related risks stemming from their supply chain.

In this context, the majority of surveyed organizations should consider fast-tracking the improvement of their capabilities related to the "IoT security training and awareness plan", "IoT supplier contract management plan", "IoT End-of-Life plan", "IoT software assets inventory", and "IoT supply chain risk assessment" controls of IoTSRM2. Moreover, to allow for better prioritization of effort, the surveyed organizations should consider improving these capabilities in tandem with their capabilities related to the "Criticality and impact analysis" of the IoTSRM2.

Weighted Results on IoTSRM2 for Surveyed Organizations

Then, Section 3.1.2 provides the key results on the entire IoTSRM2 for the surveyed organizations by outlining the degree of compliance of each of these organizations with the IoTSRM2. The IoTSRM2 compliance score for each surveyed organization resulted based on all survey responses of that surveyed organization and the IoTSRM2 adjusted control weights for each of the IoTSRM2 controls and related questions. It is worth noting that the IoTSRM2 compliance score for each surveyed organization is calculated using Equation (4) (see Section 2.2.3).

Furthermore, for each of the surveyed organizations from each of the four regions of the world considered in our IoTSRM2-based survey, Figure 14 shows the corresponding IoTSRM2 compliance score and indicates whether this score is less than 50% or greater than or equal to 50%. It is worth noting that each surveyed organization is uniquely identified using our proposed naming convention (see Section 2.2.3) which allows readers to differentiate surveyed organizations from each other and to determine the organization category and industry classification of each surveyed organization from its name.

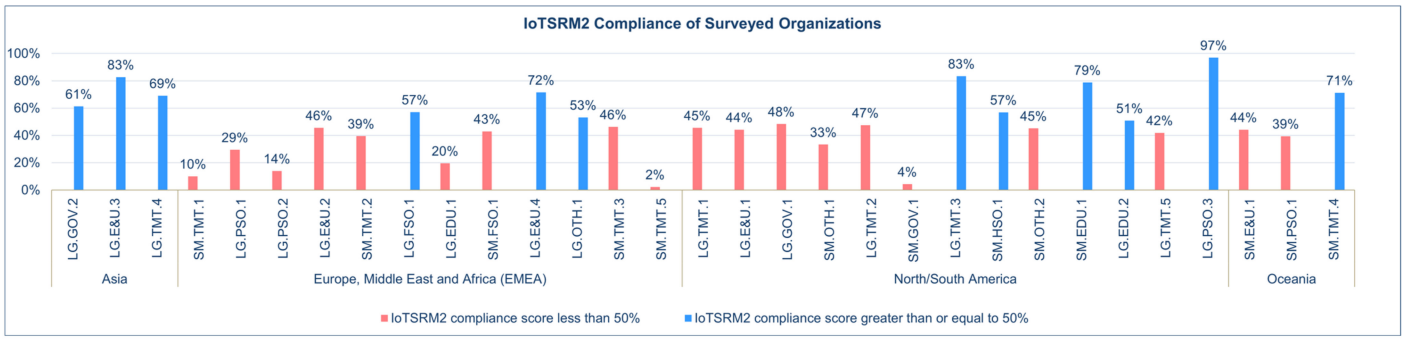

Figure 14. The IoTSRM2 compliance of surveyed organizations.

Thus, the top three highest IoTSRM2 compliance scores correspond to one large organization (i.e., LG.PSO.3) from the "North/South America" region, one large organization (i.e., LG.E&U.3) from the "Asia" region, one large organization (i.e., LG.TMT.3) from the "North/South America" region, and one small-medium organization (i.e., SM.EDU.1) from the "North/South America" region, in that order, whereas the top three lowest IoTSRM2 compliance scores correspond to one small-medium organization (i.e., SM.TMT.5) from the "Europe, Middle East and Africa (EMEA)" region, one small-medium organization (i.e., SM.GOV.1) from the "North/South America" region, and one small-medium organization (i.e., SM.TMT.1) from the "Europe, Middle East and Africa (EMEA)" region, in that order. About the surveyed organizations that have the top three highest IoTSRM2 compliance scores, these results show that except for LG.E&U.3, all organizations are from the "North/South America" region. Moreover, except for SM.EDU.1, all surveyed organi-

zations that have the top three highest IoTSRM2 compliance scores are large organizations. As for the surveyed organizations that have the top three lowest IoTSRM2 compliance scores, these results show that except for SM.GOV.1, all organizations are from the "Europe, Middle East and Africa (EMEA)" region. Moreover, all surveyed organizations that have the top three lowest IoTSRM2 compliance scores are small-medium organizations.

Furthermore, when it comes to the IoTSRM2 compliance scores across all industry sectors and regions, Figure 14 shows that half of the surveyed large organizations (i.e., LG.PSO.3, LG.TMT.3, LG.E&U.3, LG.E&U.4, LG.TMT.4, LG.GOV.2, LG.FSO.1, LG.OTH.1, and LG.EDU.2) scored greater than or equal to 50%, whereas most surveyed small-medium organizations (i.e., SM.TMT.5, SM.GOV.1, SM.TMT.1, SM.OTH.1, SM.PSO.1, SM.TMT.2, SM.FSO.1, SM.E&U.1, SM.OTH.2, and SM.TMT.3) scored less than 50%.

Then, with respect to the IoTSRM2 compliance scores for the surveyed large organizations for each industry sector irrespective of their region, Figure 14 reveals the following:

- Half of the surveyed organizations for the "Energy & Utilities" industry sector (i.e., LG.E&U.3 and LG.E&U.4) scored greater than or equal to 50%;
- Half of the surveyed organizations for the "Education" industry sector (i.e., LG.EDU.2) scored greater than or equal to 50%;
- All surveyed organizations for the "Financial & Insurance Services" industry sector (i.e., LG.FSO.1) scored greater than or equal to 50%;
- Half of the surveyed organizations for the "Government" industry sector (i.e., LG.GOV.2) scored greater than or equal to 50%;
- All surveyed organizations for the "Other" industry sector (i.e., LG.OTH.1) scored greater than or equal to 50%, most surveyed organizations for the "Professional Services" industry sector (i.e., LG.PSO.1 and LG.PSO.2) scored less than 50%;
- Most surveyed organizations for the "Technology, Media, & Telecom" industry sector (i.e., LG.TMT.2, LG.TMT.1, and LG.TMT.5) scored less than 50%.

Hence, considering the percentage of surveyed large organizations that scored IoTSRM2 compliance greater than or equal to 50% for each industry sector irrespective of their region, the surveyed large organizations for the "Financial & Insurance Services" and "Other" industry sectors scored higher than those corresponding to the remaining industry sectors.

About the IoTSRM2 compliance scores for the surveyed small-medium organizations for each industry sector irrespective of their region, Figure 14 reveals the following:

- All surveyed organizations for the "Energy & Utilities" industry sector (i.e., SM.E&U.1) scored less than 50%;
- All surveyed organizations for the "Education" industry sector (i.e., SM.EDU.1) scored greater than or equal to 50%;
- All surveyed organizations for the "Financial & Insurance Services" industry sector (i.e., SM.FSO.1) scored less than 50%;
- All surveyed organizations for the "Government" industry sector (i.e., SM.GOV.1) scored less than 50%;
- All surveyed organizations for the "Healthcare" industry sector (i.e., SM.HSO.1) scored greater than or equal to 50%;
- All surveyed organizations for the "Other" industry sector (i.e., SM.OTH.2 and SM.OTH.1) scored less than 50%;
- All surveyed organizations for the "Professional Services" industry sector (i.e., SM.PSO.1) scored less than 50%;
- Most surveyed organizations for the "Technology, Media, & Telecom" industry sector (i.e., SM.TMT.3, SM.TMT.2, SM.TMT.1, and SM.TMT.5) scored less than 50%.

Hence, considering the percentage of surveyed small-medium organizations that scored IoTSRM2 compliance greater than or equal to 50% for each industry sector irrespective of their region, the surveyed organizations for the "Education" and "Healthcare" industry sectors scored higher than those corresponding to the other industry sectors.

Furthermore, with respect to the IoTSRM2 compliance scores for the surveyed large organizations for each region regardless of their industry sector, Figure 14 shows the following:

- All surveyed organizations for the "Asia" region (i.e., LG.E&U.3, LG.TMT.4, and LG.GOV.2) scored greater than or equal to 50%;
- Most surveyed organizations for the "Europe, Middle East and Africa (EMEA)" region (i.e., LG.E&U.2, LG.PSO.1, LG.EDU.1, and LG.PSO.2) scored less than 50%;
- Most surveyed organizations for the "North/South America" region (i.e., LG.GOV.1, LG.TMT.2, LG.TMT.1, LG.E&U.1, and LG.TMT.5) scored less than 50%.

Hence, percentage-wise, more surveyed large organizations, regardless of their industry sector, scored IoTSRM2 compliance greater than or equal to 50% for the "Asia" region than for each of the other regions.

As for the IoTSRM2 compliance scores for the surveyed small-medium organizations for each region regardless of their industry sector, Figure 14 shows the following:

- All surveyed organizations for the "Europe, Middle East and Africa (EMEA)" region (i.e., SM.TMT.3, SM.FSO.1, SM.TMT.2, SM.TMT.1, and SM.TMT.5) scored less than 50%;
- Most surveyed organizations for the "North/South America" region (i.e., SM.OTH.2, SM.OTH.1, and SM.GOV.1) scored less than 50%;
- Most surveyed organizations for the "Oceania" region (i.e., SM.E&U.1 and SM.PSO.1) scored less than 50%.

Thus, percentage-wise, more surveyed small-medium organizations, regardless of their industry sector, scored IoTSRM2 compliance greater than or equal to 50% for the "North/South America" region than for each of the other regions.

3.2. Results for Surveyed Large Organizations

This subsection is structured in three subsubsections. First it provides the results for part I of our IoTSRM2-based survey on the surveyed large organizations, second it provides the results for part II of our IoTSRM2-based survey on the surveyed large organizations, and then it provides the survey results on the surveyed large organizations that operate in the Technology, Media, & Telecom (TMT) industry sector.

3.2.1. Results for Part I of Our IoTSRM2-Based Survey on Surveyed Large Organizations

This subsubsection provides our main results for part I of our IoTSRM2-based survey on the surveyed large organizations (i.e., the top organization type by surveyed organizations) including the percentage distribution of our survey respondents for large organizations by position level and the percentage distributions of the responses to our IoTSRM2-based survey for large organizations by industry sector and regions.

Furthermore, Figure 15 provides the percentage distribution of the survey respondents for surveyed large organizations by position level, which reveals that the "Consulting practice leader and/or principal" position level makes up the majority of our survey respondents for large organizations (i.e., around 56%), followed by the "C-level executive and/or board member" position level. Hence, the "Consulting practice leader and/or principal" position level of our survey respondents resulted in having the top percentage score for the surveyed large organizations by survey respondents.

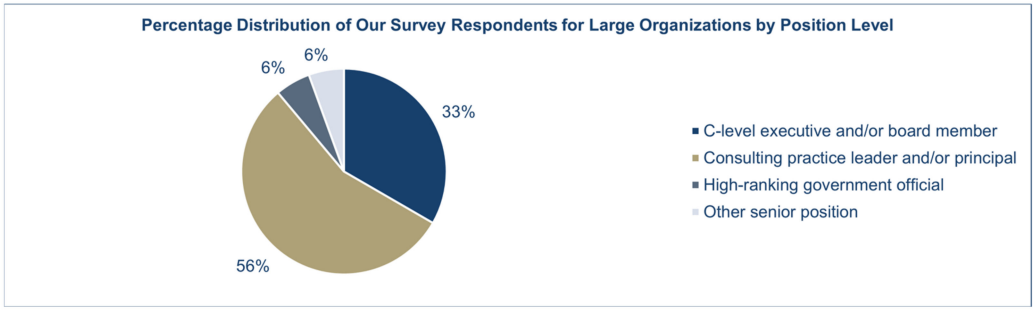

Figure 15. Distribution of our survey respondents for large organizations by position level.

Then, Figure 16 shows the percentage distribution of the survey responses for surveyed large organizations by industry classification. Hence, this figure reveals that the "Technology, Media, & Telecom (TMT)" industry sector makes up the top industry sector for the surveyed large organizations.

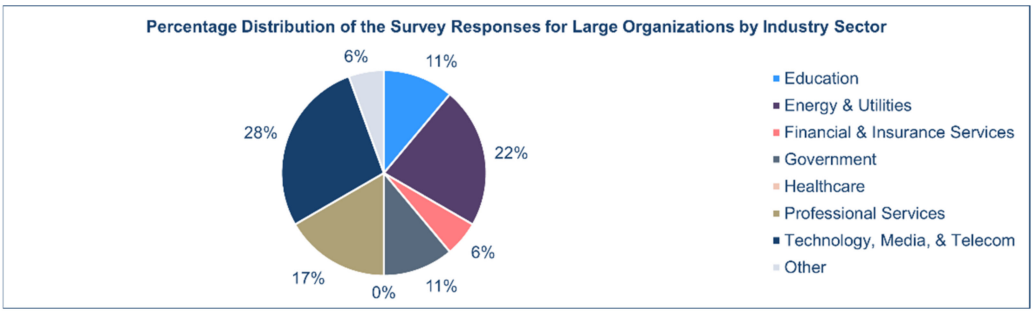

Figure 16. Distribution of survey responses for large organizations by industry classification.

Then, Figure 17 shows the percentage distribution of the surveyed large organizations by region, which reveals that most survey responses (i.e., 83%) correspond to organizations headquartered in the "North/South America" and "Europe, Middle East and Africa (EMEA)" regions. Thus, the "North/South America" region resulted in having the top percentage score (i.e., 44%) for the surveyed large organizations by survey respondents.

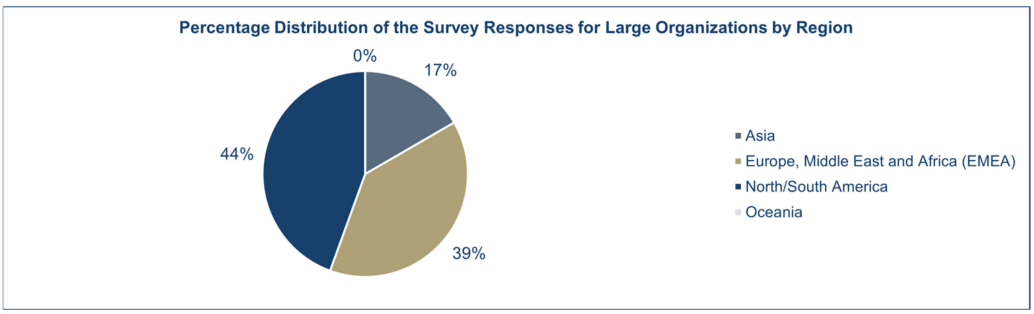

Figure 17. Distribution of survey responses for large organizations by region.

3.2.2. Results for Part II of Our IoTSRM2 Survey on Surveyed Large Organizations

This subsubsection provides our main results for part II of our IoTSRM2-based survey on the surveyed large organizations, including the weighted results on IoTSRM2 controls for the surveyed large organizations.

Weighted Results on IoTSRM2 Controls for Surveyed Large Organizations

Section 3.2.2 outlines the key results on the IoTSRM2 controls for the surveyed large organizations by outlining the overall average compliance with IoTSRM2 controls. The overall average IoTSRM2 compliance score for each IoTSRM2 control and related question

resulted based on all survey responses for surveyed large organizations and the corresponding IoTSRM2 adjusted control weight for that IoTSRM2 control and related question. It is worth noting that, for each IoTSRM2 control, the overall average IoTSRM2 compliance score is calculated using Equations (1)–(3) (see Section 2.2.3).

Furthermore, Figure 18 presents the consolidated view of the survey responses on the surveyed large organizations through the corresponding overall average IoTSRM2 compliance score for each IoTSRM2 control and related question. For each IoTSRM2 control and related question, this figure indicates whether the corresponding overall average IoTSRM2 compliance score leans towards deviating from or meeting the "as-is" IoTRSM2 control.

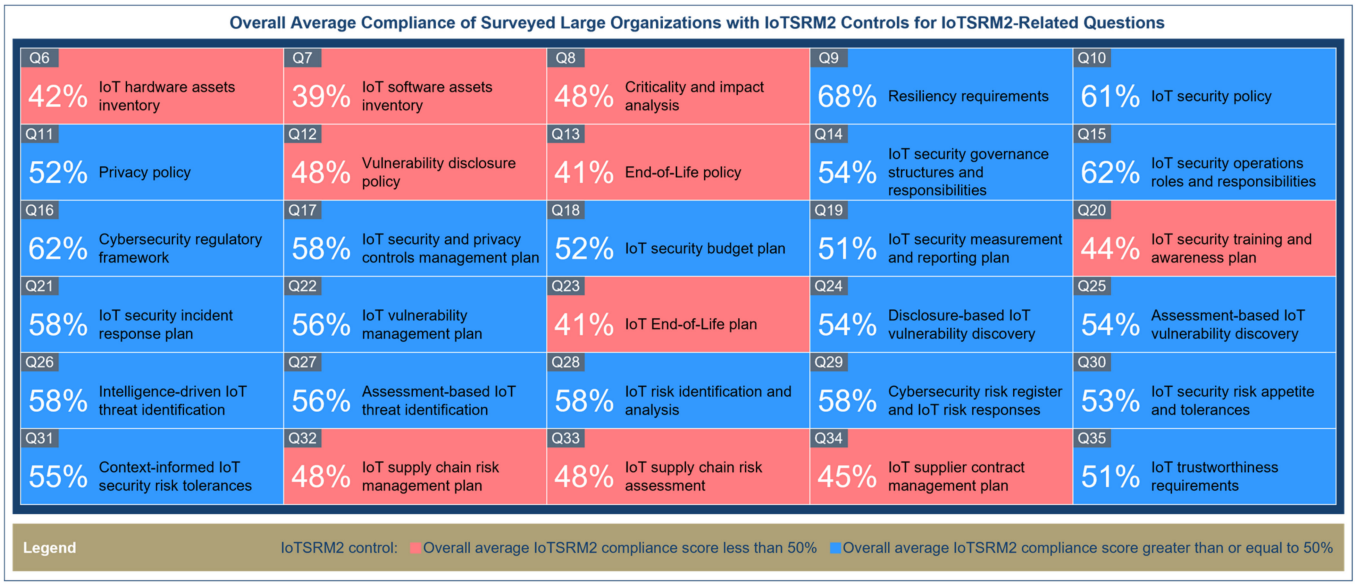

Figure 18. Overall average compliance with IoTSRM2 controls based on the survey responses for large organizations.

Figure 18 shows that the overall average IoTSRM2 compliance score across the surveyed large organizations is marginally greater than 50% for the majority of the IoTSRM2 controls and less than 50% for the remaining ten IoTSRM2 controls. Thus, the "Resiliency requirements", "IoT security operations roles and responsibilities", "Cybersecurity regulatory framework" and "IoT security policy" controls resulted in having the top three highest overall average IoTSRM2 compliance scores, in that order, whereas the "IoT software assets inventory", "IoT End-of-Life plan", "End-of-Life policy", and "IoT hardware assets inventory" controls resulted in having the top three lowest overall average IoTSRM2 compliance scores, in that order.

First, with respect to the top three highest overall average IoTSRM2 compliance scores, these findings suggest that the majority of the surveyed large organizations focus on building more resilient mission critical IoT enabled services, maintain clearly defined IoT security operations roles and responsibilities, are aware of their IoT security and privacy regulatory obligations, and have their top management's commitment towards IoT security articulated through a formal IoT security policy.

Second, regarding the top and fourth lowest overall average IoTSRM2 compliance scores, namely for the "IoT software assets inventory" and "IoT hardware assets inventory" controls, respectively, our survey results show that the majority of the surveyed large organizations do not have a comprehensive situational awareness on their IoT assets. This finding is quite worrying as it suggests that the majority of the surveyed large organizations not only they do not know their whole IoT attack surface but also may not have a clear picture of their cyber threat landscape, which may negatively impact their ability to adequately assess and manage their IoT security and privacy risks and in turn affect their ability to adequately protect their IoT infrastructures and enabled assets.

As for the second and third lowest overall average IoTSRM2 compliance scores, namely for the "IoT End-of-Life plan" and "End-of-Life policy" controls, respectively, our survey results show that the majority of the surveyed large organizations deviate or nearly deviate from the "as-is" corresponding IoTSRM2 controls. These findings of our survey suggest that the majority of the surveyed large organizations are sitting on a time bomb relative to their IoT adoptions. This is because of the security and privacy implications of ending up relying on End-of-Life IoT assets without proper in-house planning in advance and awareness of their IoT suppliers' sunsetting plans. These implications range from having unsecured hackable IoT assets lying around to experiencing life-threatening IoT failures.

Thus, the majority of surveyed large organizations should consider accelerating the improvement of their capabilities related to the "IoT software assets inventory", "IoT hardware assets inventory", "IoT End-of-Life plan", and "End-of-Life policy" controls of IoTSRM2. Moreover, to allow for better prioritization of effort, the surveyed large organizations should consider improving these capabilities in tandem with their capabilities related to the "Criticality and impact analysis" of the IoTSRM2.

3.2.3. Results for Surveyed Large Organizations from Technology, Media, & Telecom (TMT)

This subsubsection first provides our main results for part I of our IoTSRM2-based survey on the surveyed large organizations that operate in the Technology, Media, & Telecom (TMT) industry sector, and then it provides the results for part II of our IoTSRM2-based survey on the surveyed large TMT organizations, which focuses on the weighted results on IoTSRM2 controls for the surveyed large TMT organizations.

Results for Part I of Our IoTSRM2-Based Survey on Surveyed Large TMT Organizations

First, Section 3.2.3 provides the percentage distribution of our survey respondents for large TMT organizations by position level and the percentage distribution of the survey responses for large TMT organizations by region.

Thus, Figure 19 provides the percentage distribution of the survey respondents for large TMT organizations by position level, which shows that the majority of our survey respondents for large TMT organizations (i.e., 80%) correspond to and are evenly distributed across the "C-level executive and/or board member" and "Consulting practice leader and/or principal" position levels. Thus, these two position levels of our survey respondents resulted in having the top percentage score for the surveyed large TMT organizations by survey respondents.

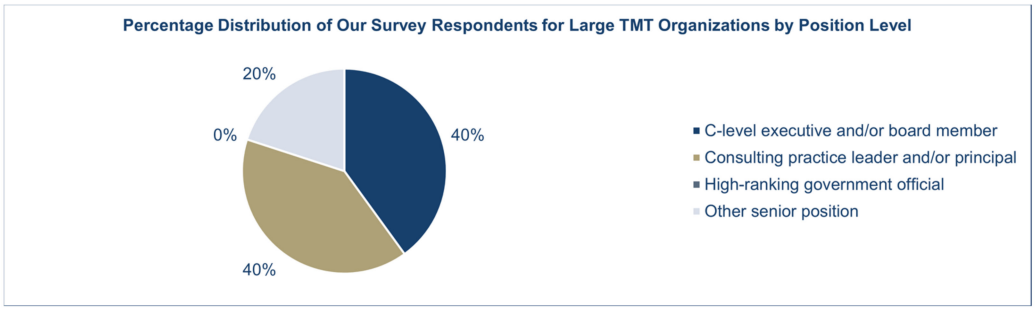

Figure 19. Distribution of our survey respondents for large TMT organizations by position level.

Then, Figure 20 shows the percentage distribution of the surveyed large TMT organizations by region, which reveals that most survey responses for large TMT organizations (i.e., 80%) correspond to organizations headquartered in the "North/South America" region. Hence, the "North/South America" region resulted in having the top percentage score for the surveyed large TMT organizations by survey respondents.

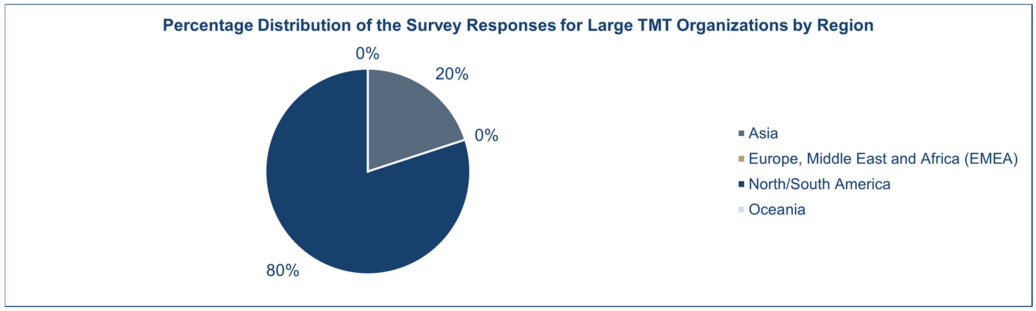

Figure 20. Distribution of survey responses for large TMT organizations by region.

Results for Part II of Our IoTSRM2-Based Survey on Surveyed Large TMT Organizations

Second, Section 3.2.3 outlines the key results on the IoTSRM2 controls for the surveyed large TMT organizations by outlining the overall average compliance with IoTSRM2 controls. The overall average IoTSRM2 compliance score for each IoTSRM2 control and related question resulted based on all survey responses for surveyed large TMT organizations and the corresponding IoTSRM2 adjusted control weight for that IoTSRM2 control and related question. It is worth noting that, for each IoTSRM2 control, the overall average IoTSRM2 compliance score is calculated using Equations (1)–(3) (see Section 2.2.3).

Furthermore, Figure 21 presents the consolidated view of the survey responses on the surveyed large TMT organizations through the corresponding overall average IoTSRM2 compliance score for each IoTSRM2 control and related question. For each IoTSRM2 control and related question, this figure indicates whether the corresponding overall average IoTSRM2 compliance score leans towards deviating from or meeting the "as-is" IoTRSM2 control.

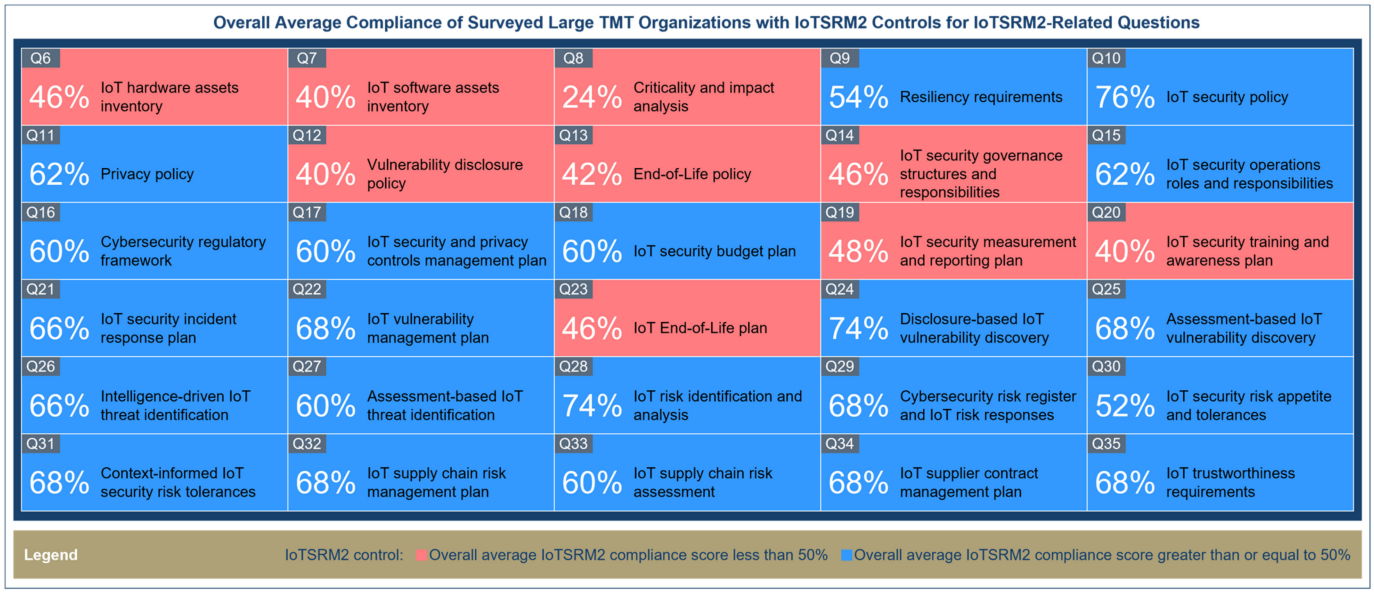

Figure 21. Overall average compliance with IoTSRM2 controls based on the survey responses for large TMT organizations.

Figure 21 shows that the overall average IoTSRM2 compliance score across the surveyed large TMT organizations is greater than 50% for the majority of the IoTSRM2 controls and less than 50% for the other nine IoTSRM2 controls. Hence, the "IoT security policy", "Disclosure-based IoT vulnerability discovery", "IoT risk identification and analysis", "IoT vulnerability management plan", "Assessment-based IoT vulnerability discovery", "Context-informed IoT security risk tolerances", "IoT trustworthiness requirements", "Cybersecurity risk register and IoT risk responses", "IoT supply chain risk management plan", and "IoT supplier contract management plan" controls resulted in having the top three highest overall average IoTSRM2 compliance scores, in that order, whereas the "Criticality and impact analysis", "Vulnerability disclosure policy", "IoT software assets inventory", and "IoT security training and awareness plan" controls resulted in having the top three lowest overall average IoTSRM2 compliance scores, in that order.

First, with respect to the top three highest overall average IoTSRM2 compliance scores, our survey results reveal that the majority of the surveyed large TMT organizations have their senior management's commitment towards IoT security clearly articulated through a formal IoT security policy, adopt proactive risk assessment approaches fueled by IoT vulnerability management, and understand the importance of maintaining their preparedness for facing IoT supply chain risk related events.

Then, about the "Criticality and impact analysis" control, our survey result reveals that most surveyed large TMT organizations deviate or nearly deviate from the "as-is" corresponding IoTSRM2 control. Thus, although most of the surveyed large TMT organizations adopt proactive risk assessment approaches, this survey result suggests that many or at least some of these organizations address IoT risks in most cases using one-size-fits-all IoT security risk management approaches which could have catastrophic consequences. For instance, catastrophic consequences could turn up in the event of a life-threatening IoT risk occurrence while having implemented hugely disproportionate countermeasures across the board to effectively address this IoT risk.

With respect to the "Vulnerability disclosure policy" control, although the majority of the surveyed large TMT organizations engage in IoT supply chain risk management, our finding shows that most of these organizations contract IoT suppliers that either do not have an up-to-date vulnerability disclosure policy or do not communicate it well enough to them. Moreover, considering that most surveyed large TMT organizations leverage vulnerability disclosures as part of their risk assessment processes, this survey finding further suggests that these organizations establish vulnerability handling processes

with their IoT suppliers ahead of contracting. Notwithstanding, the absence of a publicly available vulnerability disclosure policy may translate for these large TMT organizations in not being able to avail of timely IoT patches and in turn having unpatched, hackable IoT technologies in use due to lags in third party IoT vulnerability reporting.

Furthermore, with respect to the "IoT software assets inventory" control, our survey result shows that the majority of the surveyed large TMT organizations do not have an all-encompassing picture of all their IoT software assets, which further indicates that these organizations may be exposed to shadow IoT software. Moreover, considering that our survey finding shows that some of these organizations are also unaware of all their IoT hardware assets, these large TMT organizations should consider better dealing with inventorying their IoT assets to reduce the likelihood of bad thinks happening. It is worth noting that shadow IoT risk may have a cascading effect on the performance of the IoT risk assessment processes if it materializes.

As for the "IoT security training and awareness plan" control, our survey result reveals that most of the surveyed large organizations deviate or nearly deviate from the "as-is" corresponding IoTSRM2 control. This survey finding suggests that the majority of the surveyed large TMT organizations are unaware of or do not clearly grasp their IoT security and privacy risks, which in turn may favor scenarios where these organizations are breached due to lack of IoT risk awareness.

Thus, the majority of the surveyed large TMT organizations should consider boosting the pace of the improvement of their capabilities related to the "Criticality and impact analysis", "Vulnerability disclosure policy", "IoT software assets inventory", and "IoT security training and awareness plan" controls of the IoTSRM2.

4. Related Work

A sizeable number of academic and industry research studies has been published on IoT security [14]. However, at the time of writing, no research study was found to exclusively focus on determining the current state of IoT security risk management strategies in organizations. Hence, given there are numerous research studies in the literature relevant to IoT security, this section encompasses the related work to our IoTSRM2-related survey study and covers the related works that meet the following three selection criteria and one condition:

- **Selection criterion 1:** The related work is available in English;
- **Selection criterion 2:** The related work is focused on determining the current state of IoT security risk management strategy in organizations at least to a certain extent;
- **Selection criterion 3:** The related work employs an interview-, survey-, or experiment-based research method;
- **Condition 1:** The related works are research studies from both academia and industry.

Thus, Table 9 lists the 12 selected related works for our evaluation, and it outlines the following details: the current row number (i.e., "No."), the author/publisher of the related research study (i.e., "Author/Publisher"), the title of the research work (i.e., "Title"), and the corresponding reference (i.e., "Reference").

Table 9. Selected related works.

No.	Author/Publisher	Title	Reference
1.	Palo Alto Networks	2020 Unit 42 IoT Threat Report	[15]
2.	The Ponemon Institute	A New Roadmap for Third Party IoT Risk Management the Critical Need to Elevate Accountability, Authority and Engagement	[19]
3.	Almutairi and Almarhabi	Investigation of Smart Home Security and Privacy: Consumer Perception in Saudi Arabia	[31]
4.	Arm Limited	Bridging the Gap PSA Certified Security Report 2021 How collaboration will secure the future of IoT	[32]
5.	Asplund and Nadjm-Tehrani	Attitudes and Perceptions of IoT Security in Critical Societal Services	[33]
6.	The Cabinet Office	Consumer Attitudes Towards IoT Security	[34]
7.	Forescout Technologies	The Enterprise of Things Security Report the State of IoT Security	[35]
8.	Gemalto	The State of IoT Security	[36]
9.	IBM	Electronics Industrial IoT cybersecurity	[37]
10.	Juniper Networks	Securing IoT at Scale Requires a Holistic Approach Survey Insights Revealed by IoT Adopters	[38]
11.	The SANS Institute	The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns	[39]
12.	UL	Security concerns escalate as IoT expands Market insights on the state of IoT security	[40]

Then, this section covers the analysis of the 12 selected related works. Thus, with respect to the analysis of the literature related to our IoTSRM2-based survey study, Table 10 shows the IoTSRM2-based survey study together with the 12 reviewed related works mapped against the proposed evaluation criteria and the extent of applicability to each evaluation criterion. With respect to the proposed evaluation criteria, seven evaluation criteria were formulated based on our proposed methodology for determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2 (see Section 2.2). Moreover, with respect to the extent of applicability, three types of applicability were considered relevant to indicate differences and/or similarities between this IoTSRM2-based survey study and the in-scope research works for this evaluation.

Table 10. The IoTSRM2-based survey study and related work mapped to evaluation criteria and extent of applicability.

Evaluation Criterion	Extent of Applicability		
	The Evaluation Criterion Fully Applies	**The Evaluation Criterion Applies to a Certain Extent**	**The "as-Is" Evaluation Criterion Does Not Apply**
E1: The research study is focused on determining the current state of IoT security risk management strategies in organizations	Our IoTSRM2-based survey study	[15,19,31–40]	None of these related works
E2: The methodology for achieving the intended purpose of the research study is clearly described	[35], Our IoTSRM2-based survey study	[15,31–34]	[19,36–40]
E3: The underlying design best practice of the research method of the methodology is clearly documented	Our IoTSRM2-based survey study	[33]	[15,19,31,32,34–40]
E4: Provides results for organizations of a specific organization size	[32,36,39], Our IoTSRM2-based survey study	None of these related works	[15,19,31,33–35,37,38,40]
E5: Provides results for organizations from a specific industry sector	[15,35,37,40], Our IoTSRM2-based survey study	None of these related works	[19,31–34,36,38,39]
E6: The results reveal the level of compliance of each subject with a reference model	Our IoTSRM2-based survey study	[39]	[15,19,31–38,40]
E7: The findings resemble the results of our IoTSRM2-based survey	Our IoTSRM2-based survey study	[15,19,32,36–40]	[31,33–35]

Afterwards, this section presents the evaluation of this IoTSRM2-based survey study and the 12 reviewed related works for each evaluation criterion.

E1: The research study is focused on determining the current state of IoT security risk management strategies in organizations

None of the reviewed related works focused on determining the current state of IoT security risk management strategies in organizations. However, the 12 reviewed related works addressed this issue to a certain extent by focusing on determining the current state of IoT security in organizations (i.e., [15,32,33,35,36,38,40]), of Industrial IoT (IIoT) security in organizations (i.e., [37,39]), of IoT security for consumers (i.e., [31,34]) and of third party IoT risk management in organizations (i.e., [19]).

With respect to the seven reviewed related works that focused on determining the current state of IoT security in organizations, these related works focused their studies on understanding IoT security challenges and opportunities, threats, risks, capabilities and enablers, and investment priorities. Thus, first, Palo Alto Networks [15] evaluated the state of the IoT threat landscape by using data from real deployments. Second, Arm Limited [32] focused their study on understanding the IoT security challenges and opportunities from the surveyed organizations. Third, Asplund and Nadjm-Tehrani [33] investigated the attitudes and perceptions among interviewed industry actors on IoT security in critical societal services. Fourth, Forescout Technologies [35] provided the state of enterprise IoT network security of some of their customer deployments within and across industry verticals by looking at enterprise network threat and risk exposure. Then, Gemalto [36] provided the IoT security state in surveyed organizations by looking at the IoT security capabilities of and the use of blockchain technology to secure IoT data, services, and devices in surveyed organizations. Afterwards, as part of the Juniper Networks white paper on IoT

security, Juniper Networks [38] reported on the IoT security risks, challenges, capabilities, and investment priorities of surveyed organizations that have implemented IoT projects. Finally, UL [40] focused their survey study on determining how the organizations are preparing for and responding to the current and emerging IoT security threats.

Then, about the two reviewed related works that focused on determining the current state of IIoT security in organizations, IBM [37] determined the IIoT security risks and their implications for the surveyed organizations from the energy and industrial sectors, and the SANS Institute [39] investigated the capabilities, threats, and risks of IIoT security in surveyed organizations.

With respect to the two reviewed related works that focused on determining the current state of IoT security for consumers, Almutairi and Almarhabi [31] studied the security and privacy concerns of their survey respondents about the smart home devices in the Saudi Arabia, and the Cabinet Office [34] investigated the consumer attitudes towards IoT security.

Furthermore, the Ponemon Institute [19] focused on determining the current state of third party IoT risk management in surveyed organizations.

Compared with these 12 reviewed related works, our IoTSRM2-based survey study is focused on determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2.

E2: The methodology for achieving the intended purpose of the research study is clearly described

Our proposed three-phased methodology for achieving the intended purpose of this IoTSRM2-based survey study, namely determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2, is clearly described (see Section 2.2). Our methodology includes nine steps and outputs related to the plan and create, launch and run, and analyze and report phases.

Furthermore, from the 12 reviewed related works, one of them clearly described the methodology used for achieving the intended purpose of the research study (i.e., [35]), five of them partially described their methodology (i.e., [15,31–34]), while the remaining ones did not describe their methodology (i.e., [19,36–40]).

Regarding the related work that clearly described its methodology, Forescout Technologies [35] provided the methodology applied for determining the state of enterprise IoT network security of some of their customer deployments by outlining three main steps, namely data collection, data cleaning and enrichment, and data analysis. Furthermore, Forescout Technologies [35] provided details about the risk score model created and used to measure the risk values for all IoT devices of some of their customer deployments, which were then used to analyze the anonymous enterprise device data from the Forescout Device Cloud. In contrast with the research work performed by Forescout Technologies [35] which entails an experimental study that processes data from some of their customer deployments, our proposed methodology from this article involves a survey-based study that leverages the survey data drawn from the survey respondents on the surveyed organizations. Although our proposed methodology from this article has different objectives than the study conducted by Forescout Technologies [35], similar to the methodology of Forescout Technologies [35] which includes, among others, data collection, data cleaning, and data analysis steps for anonymous data, our proposed three-phased methodology includes, among others, steps that entail the collection, cleaning and analysis of anonymous data as part of the launch and run, and analyze and report phases.

Furthermore, from the perspective of the extent of applicability to this evaluation criterion, our proposed methodology differentiates from the methodologies provided by Palo Alto Networks [15], Almutairi and Almarhabi [31], Arm Limited [32], Asplund and Nadjm-Tehrani [33], and the Cabinet Office [34], as it is much more detailed than the ones of these five reviewed related works which offer limited details. Thus, first, Palo Alto Networks [15] provided merely some details about their experimental setup and data gathering rather than describing the analysis and reporting activities of the data collected from their

customers. Second, Almutairi and Almarhabi [31] developed the questionnaire used for running the survey and provided details on how their questionnaire was developed. However, Almutairi and Almarhabi [31] provided limited details on how the survey planning and creation were performed and did not clearly outline the ways in which the analysis and reporting of survey responses were carried out. Third, Arm Limited [32] provided limited details about their methodology including the use of the Sapio Research online panel for conducting the survey, the usage of email invitations, and the distribution channels used for requesting survey participation. In this context, the methodology provided by Arm Limited [32] does not outline how the questionnaire is developed, how the survey is designed, and how the analysis and reporting of survey responses are performed. Fourth, Asplund and Nadjm-Tehrani [33] described the methodology for their interview-based study only half-way as it provides details about the type of questions used, the design of the questionnaire, the selection of the respondents, and the reporting format (i.e., through quotes) without describing the data collection and analysis activities. Finally, the Cabinet Office [34] provided limited details on their methodology and reported the use of the Ipsos MORI online panel for running their survey, the incentive used for attracting more survey participants, and the details concerning the request for survey participation. However, the Cabinet Office [34] did not provide details on how the questionnaire was developed, how the survey was designed, and how the analysis and reporting of survey responses were performed.

E3: The underlying design best practice of the research method of the methodology is clearly documented

As per Table 10, none of the 12 reviewed related works clearly documented the design best practice on which the research method of their methodology is based. However, Asplund and Nadjm-Tehrani [33] documented their own principles guiding the questionnaire design for their interview-based study, which are not based on a well renowned reference source. Compared with the 12 reviewed related works, our IoTSRM2-based survey study relies on the principles for designing web questionnaires developed by Dillman et al. [20], and the applicability of these principles to our IoTSRM2-based survey is clearly documented as part of Table 5.

E4: Provides results for organizations of a specific organization size

Our IoTSRM2-based survey study reports the percentage distribution of the surveyed organizations by organization category/type (i.e., based on the organization size) (see Section 3.1.1), the IoTSRM2 compliance score of each of the surveyed organizations together with indicating the category/type (i.e., based on size) of that organization (see Section 3.1.2), and the IoTSRM2-based survey results on the surveyed large organizations (see Section 3.2). In addition, from the 12 reviewed related works, three of them provided results for organizations of a specific organization size (i.e., [32,36,39]), whereas the remaining ones did not provide any results for organizations of a specific organization size (i.e., [15,19,31,33–35,37,38,40]).

Regarding the three reviewed related works that provided results for organizations of a specific organization size, Arm Limited [32] provided some of their results for small organizations and for large organizations (e.g., threat modelling adoption, satisfaction with IoT security expertise), Gemalto [36] provided all their results for large organizations having an employee headcount of more than 250, and the SANS Institute [39] provided some of their results by organization size (e.g., number of connected IoT devices).

E5: Provides results for organizations from a specific industry sector

Our IoTSRM2-based survey study provides the percentage distribution of the surveyed organizations by industry classification/sector (see Section 3.1.1), the IoTSRM2 compliance score of each of the surveyed organizations together with indicating the industry sector of that organization (see Section 3.1.2), the percentage distribution of the surveyed large organizations by industry classification/sector (see Section 3.2.1), and the IoTSRM2-based survey results on the surveyed large TMT organizations (see Section 3.2.3). In addition, from the 12 reviewed related works, four of them provided some of their survey results for organizations from a specific industry sector (i.e., [15,35,37,40]), whereas

the remaining ones did not provide any results for organizations from a specific industry sector (i.e., [19,31–34,36,38,39]).

With respect to the four reviewed related works that provided results for organizations from a specific industry sector, Palo Alto Networks [15] provided their results for the enterprise IT and healthcare industry sectors and some of these results are mainly focused on the organizations from the healthcare industry sector, Forescout Technologies [35] provided all their findings for specific industry verticals, IBM [37] provided all their results for the electronics industry sector, and UL [40] provided some of their results for organizations from specific industry sectors (e.g., IoT security plan).

E6: The results reveal the level of compliance of each subject with a reference model

As per Table 10, none of the 12 reviewed related works provided results that reveal the level of compliance of the subjects with a reference model. However, the SANS Institute [39] meets this evaluation criterion to a certain extent. This is because the SANS Institute [39] provided merely the overall results for their survey respondents that indicate percentage scores of the IIoT devices connecting to different levels and zones of the network infrastructure following the Purdue model hierarchy rather than reporting the level of compliance of each subject with the Purdue model. Compared with the 12 reviewed related works, our IoTSRM2-based survey study outlines the degree of compliance of each of the surveyed organizations with the IoTSRM2 (see Section 3.1.2) and provides the IoTSRM2 compliance score for each of the surveyed organizations (see Figure 14).

E7: The findings resemble the results of our IoTSRM2-based survey

This article provides our IoTSRM2-based survey results for each of the three groups of surveyed organizations (i.e., the surveyed large and small-medium organizations, the surveyed large organizations, and the surveyed large TMT organizations). As per Table 10, none of the reviewed related works reported findings that fully resemble the results of our IoRSRM2-based survey. However, eight of the reviewed related works, namely Palo Alto Networks [15], the Ponemon Institute [19], Arm Limited [32], Gemalto [36], IBM [37], Juniper Networks [38], the SANS Institute [39], and UL [40], reported one or more findings that resemble some of our survey results, while the remaining ones (i.e., [31,33–35]) did not report any findings that resemble our survey results.

With respect to the eight reviewed related works that meet this evaluation criterion to a certain extent, the Ponemon Institute [19] reported five findings, Palo Alto Networks [15], Arm Limited [32] and the SANS Institute [39] each reported four findings, Gemalto [36] and IBM [37] each reported two findings, and the remaining two research studies (i.e., [38,40]) reported one finding that resemble some of our survey results.

Hence, with respect to the study conducted by the Ponemon Institute [19], it reported five findings that resemble four of the weighted results of our IoTSRM2-based survey on the IoTSRM2 controls for the surveyed organizations (see Section 3.1.2). First, the long-term barrier reported by the Ponemon Institute [19], namely that organizations should consider nurturing more robust risk cultures internally around their IoT environment, reflects our survey result related to the "IoT security training and awareness plan" control of the IoTSRM2 (see Figure 13). Second, the finding reported by the Ponemon Institute [19] that very few organizations actively engage in third party IoT security audits is in line with our survey result on the "IoT supplier contract management plan" control of the IoTSRM2 (see Figure 13). Third, the finding reported by the Ponemon Institute [19] on IoT applications inventory, namely the prevalent issue of maintaining a comprehensive and relevant inventory of IoT applications, reflects our survey result on the "IoT software assets inventory" control of the IoTSRM2 (see Figure 13). Finally, the two findings reported by the Ponemon Institute [19] on resource allocation, namely the budget and staffing shortfalls to manage third party IoT risks, reflect our survey result on the "IoT supply chain risk assessment" control of the IoTSRM2 (see Figure 13).

Then, regarding the study carried out by Palo Alto Networks [15], it reported four findings that resemble four of our survey results on the IoTSRM2 controls for the surveyed organizations (see Section 3.1.2). First, the finding reported by Palo Alto Networks [15]

that organizations lack IoT device inventory is in line with our survey result on the "IoT hardware assets inventory" control of the IoTSRM2 (see Figure 12). Second, the finding reported by the Palo Alto Networks [15] that medical IoT devices run on outdated and End of Life operating systems is in line with our survey result on the "IoT End-of-Life plan" control of the IoTSRM2 (see Figure 12). Third, the finding reported by the Palo Alto Networks [15] about the necessity of an effective IoT security strategy for managing IoT risk proactively, resembles our survey result that most of our surveyed organizations underperform in strategizing governance and risk management for their IoT infrastructures (i.e., except for vulnerability management) (see Figure 12). Third, the finding reported by the Palo Alto Networks [15] that most organizations do not manage the risk profiles of their IoT devices is somehow in line with our survey result that most of our surveyed organizations are not so much engaged in all-encompassing IoT threat profiling activities, which corresponds to the "Assessment-based IoT threat identification" control of the IoTSRM2 (see Figure 12).

Afterwards, regarding the study conducted by Arm Limited [32], it reported one finding that resembles one of our survey results on the IoTSRM2 controls for the surveyed organizations, one finding that resembles one of our survey results on the IoTSRM2 compliance score of each of the surveyed organizations, and two findings that somehow resemble one of our survey results on the IoTSRM2 controls for the surveyed organizations (see Section 3.1.2). First, the second top IoT security challenge reported by Arm Limited [32], namely the lack of IoT security understanding and expertise, reflects our survey result related to the "IoT security training and awareness plan" control of the IoTSRM2 (see Figure 12). Second, the finding reported by Arm Limited [32] that IoT security implementation scales with the size of the organization is in line with our survey finding 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 (see Figure 14). Third, the findings reported by Arm Limited [32] that the majority of their survey respondents (i.e., 53%) are not carrying out threat analysis for all the IoT products they provide, and that nearly all of their survey respondents (i.e., 86%) are likely to do or redo the threat analysis in the postmarket phase of the IoT products they provide, are somehow related to our survey result on the "Assessment-based IoT threat identification" control of the IoTSRM2 in the context of perhaps having surveyed organizations that work with IoT suppliers that are not so much engaged in performing thorough IoT threat profiling activities (see Figure 12).

Then, about the study conducted by the SANS Institute [39], it reported two findings that resemble three of our survey results on the IoTSRM2 controls for the surveyed organizations, and two findings that somehow resemble two of our survey results on the IoTSRM2 controls for the surveyed organizations (see Section 3.1.2). First, the finding reported by the SANS Institute [39] that most of their respondents (i.e., 59%), regardless of organization size, need additional education and training to manage security of IIoT device, is in line with our survey result on the "IoT security training and awareness plan" control of the IoTSRM2 (see Figure 12). Second, the finding reported by the SANS Institute [39] that only 41.1% of their respondents have physical and logical inventory of connected devices to protect against IIoT risks, reflect our survey results on the "IoT hardware assets inventory" and "IoT software assets inventory" controls of the IoTSRM2 (see Figure 12). Third, the top IIoT challenge reported by the SANS Institute [39], namely the difficulty in or lack of patching for IIoT systems is somehow related to our survey result on the "Vulnerability disclosure policy" control of the IoTSRM2 from the perspective that relying on an inadequate or absent vulnerability disclosure policy may favor scenarios where vulnerable IoT systems stay unpatched for longer periods of time (see Figure 12). Fourth, the third top IIoT challenge reported by the SANS Institute [39], namely the difficulty in identifying and managing IIoT connectivity to critical infrastructure and other mission-critical systems is somehow related to our survey result on the "Criticality and impact analysis" control of the IoTSRM2 considering that managing IoT interdependencies is cumbersome and inefficient without having all IoT enabled services and enablers prioritized based on their criticality.

Furthermore, with respect to the study undertaken by Gemalto [36], it reported one finding that resembles one of our survey results on the IoTSRM2 controls for the surveyed large organizations (see Section 3.2.1), and another that somehow resembles one of our weighted survey results on the IoTSRM2 controls for the surveyed large organizations (see Section 3.2.2). First, considering that the organization size of all survey respondents of Gemalto [36] is greater than 250 employees and corresponds to the surveyed large organizations of our IoTSRM2-based survey study (see Section 2.2), the finding reported by Gemalto [36] that the "IT, technology and telecoms" is the top organization sector by survey respondents reflects our survey result on the top industry sector for the surveyed large organizations by survey respondents, namely the "Technology, Media, & Telecom (TMT)" industry sector (see Figure 16). Second, the finding reported by Gemalto [36] that the majority of their survey respondents that supply IoT products or services (i.e., 54%) increased their IoT security offerings is somehow related to our survey result on the "IoT trustworthiness requirements" control of the IoTSRM2 from the perspective that having better IoT trustworthiness requirements for the IoT supplier contracts may demand and stimulate greater IoT security offerings on the supply side (see Figure 18).

Subsequently, about the study performed by IBM [37], it reported one finding that resembles one of our weighted survey results on the IoTSRM2 controls for the surveyed large TMT organizations, and another that somehow resembles and ramifies into three of our weighted survey results on the IoTSRM2 controls for the surveyed large TMT organizations (see Section 3.2.3). First, the finding reported by IBM [37] on the inventoried authorized and unauthorized IIoT software reveals that under half of the majority of their surveyed electronics organizations control IoT software assets inventory, and it reflects our survey result on the "IoT software assets inventory" control of the IoTSRM2 (see Figure 21). Second, the finding reported by IBM [37] on the secure IIoT devices reveals that for virtually all their surveyed electronics organizations, engaging in continuous coordinated patching of IIoT devices is hard and very problematic when it comes to older legacy devices (e.g., End of Life legacy devices), and it somehow reflects our survey results on "Vulnerability disclosure policy", "End-of-Life policy", and "IoT End-of-Life plan" controls of the IoTSRM2 considering that the absence or the inadequacy of these three controls may have different repercussions on the organizations relying on them ranging from having unpatched and unsecure IoT devices to being hacked (see Figure 21).

Furthermore, with respect to the study undertaken by Juniper Networks [38], it reported one finding that resembles one of our survey results on the IoTSRM2 controls for the surveyed organizations (see Section 3.1.1). Hence, the finding reported by Juniper Networks [38] that the "Information Technology" and "Telecommunications" industry sectors make up the top industry classification for their surveyed organizations reflects our survey result on the top industry sector for the surveyed organizations by survey respondents, namely the "Technology, Media, & Telecom (TMT)" industry sector (see Figure 10).

Finally, about the study conducted by UL [40], it reported one finding that resembles one of our survey results on the IoTSRM2 controls for the surveyed organizations (see Section 3.1.2). Hence, the finding reported by UL [40] that the majority of their surveyed organizations (i.e., 77%) plan to increase spending in IoT security is in line with our survey result on the "IoT security budget plan" control of the IoTSRM2 (see Figure 12).

5. Conclusions and Future Work

This article presented our findings following the undertaking of an IoTSRM2-based survey study. These findings rely on the survey responses of leaders from industries and governments from around the world, show the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2, and aim to support IoT security practitioners to peer benchmark and enhance their IoT security risk management strategies.

First, this article introduced the acute need for robust IoT security risk management strategies in organizations embracing IoT technologies, provided the rationale for perform-

ing the IoTSRM2-based survey study, enumerated the research questions, highlighted the main contributions of our research work, outlined the structure of the article, and provided a reading map for our research questions.

Then, the article described our proposed three-phased methodology for addressing the research questions by describing the nine steps of this methodology and their associated outputs. Thus, first, the article described the three steps of the first phase (i.e., the "Plan and Create" phase) which allowed, among others, the definition of the methodology objectives, the design and creation of the IoTSRM2-based survey, and development of our survey analysis plan. Afterwards, it described the three steps of the second phase (i.e., the "Launch and Run" phase) which enabled, inter alia, the identification of the target survey respondents, the submission of survey participation requests, and the collection of survey responses. Next, it described the three steps of the third phase (i.e., the "Analyze and Report" phase) which allowed, among others, the analysis of survey responses and the reporting of survey findings.

Subsequently, the article presented our survey results for the three groups of surveyed organizations (i.e., the surveyed large and small-medium organizations, the surveyed large organizations, and the surveyed large TMT organizations).

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, our results revealed that the "Large Organization" category is the top organization type for these organizations. Third, our 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, our 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. Then, about the overall average IoTSRM2 compliance score of these organizations for each IoTSRM2 control, our 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. As for the IoTSRM2 compliance score of each of these organizations, our results revealed, 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.

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, our results showed that the "Technology, Media, & Telecom (TMT)" industry sector is the top industry sector for these organizations. Third, our 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, our 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.

Furthermore, about the results for the surveyed large TMT organizations, first, our 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, our 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, our 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.

Furthermore, this article outlined 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 selected 12 related research studies based on three selection criteria and one condition. Third, it discussed our IoTSRM2-based survey study in relation to the selected related studies using seven evaluation criteria based on our methodology and using three types of applicability to each evaluation criterion. For instance, about the evaluation criterion on the research studies that provide findings that resemble the results of our IoTSRM2-based survey study, none and eight of the reviewed related works were found to meet this criterion fully and partially, respectively.

Future work may include several projects such as extending our existing research work to further explore the surveyed small-medium organizations and the surveyed large organizations from the second top industry sector for the surveyed organizations (i.e., "Energy & Utilities"), performing IoTSRM2-based assessments of individual organizations and benchmarking their IoT security postures against our IoTSRM2-based survey findings, and redoing the IoTSRM2-based survey after a certain time to compare survey results.

Author Contributions: Conceptualization, T.M.P.; methodology, T.M.P. and A.M.P.; survey setup, T.M.P. and A.M.P.; validation, T.M.P. and A.M.P.; formal analysis, T.M.P. and A.M.P.; investigation, T.M.P. and A.M.P.; resources, T.M.P. and A.M.P.; data curation, T.M.P. and A.M.P.; writing—original draft preparation, T.M.P. and A.M.P.; writing—review and editing, T.M.P., A.M.P., and G.P.; visualization, T.M.P. and A.M.P.; supervision, T.M.P. and A.M.P.; project administration, T.M.P. and A.M.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Ethical review and approval were waived for this study due to the anonymous nature of this survey.

Informed Consent Statement: Respondent consent was waived due to the anonymous nature of this survey.

Data Availability Statement: Data available on request from the authors.

Acknowledgments: The authors would like to extend many thanks to all the people that participated in our IoTSRM2-based survey and/or diffused our IoTSRM2-based survey to reach wider audiences.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Our mapping for possible items of interest from this article.

No.	Possible Item of Interest	Our Mapping			
		Section	Presentation Mode [1]	Main Justification	Indicative Links
1.	Research gap	1. Introduction	Text only	For advancement of research	Sections 2–5
2.	Research purpose	1. Introduction	Text only	To state the significance of our research	Sections 2–5
3.	Research questions	1. Introduction	Bullet points	To provide our research directions	Section 1: Figure 2 Section 2.2.1: Table 7 Section 2.2.3: Step III.2 Sections 3–5
4.	Main contributions	1. Introduction	Bullet points	To show the significance of our research	Sections 2–4
5.	Article structure	1. Introduction	Figure 1	To enhance the readability of our article	Sections 1–5
6.	A reading map for research questions	1. Introduction	Figure 2	To enhance the readability of our article	Sections 1–5
7.	Illustrative view of IoTSRM2	2.1. Overview of Our IoTSRM2	Figure 3	To inform about our IoTSRM2	Section 3.1.2: Figures 12 and 13 Section 3.2.2: Figure 18 Section 3.2.3: Figure 21
8.	IoTSRM2 controls with adjusted weights	2.1. Overview of Our IoTSRM2	Table 1	To inform about our IoTSRM2	Section 2.2.1: Table 3 Section 3.1.2: Figures 12 and 13 Section 3.2.2: Figure 18 Section 3.2.3: Figure 21
9.	Survey methodology	2.2. Our Survey Methodology	Figure 4	To explain our research approach	Sections 1, 2.1 and 3–5
10.	Methodology objectives	2.2.1. Phase I: Plan and Create	Bullet points	To provide structure and directions for our research	Sections 1, 2.2, 3 and 4
11.	Assumptions and limitations	2.2.1. Phase I: Plan and Create	Bullet points	To inform about assumptions and limitations	Sections 2.2 and 3
12.	Part I of the questionnaire	2.2.1. Phase I: Plan and Create	Table 2	To address Objectives 3, 4, and 9	Section 2.2.1: Table 7 Section 2.2.3: Figures 5 and 6 Section 3: Figure 7 Section 3.1.1: Figures 10 and 11 Section 3.2.1: Figures 15–17 Section 3.2.3: Figures 19 and 20

Table A1. *Cont.*

No.	Possible Item of Interest	Our Mapping			
		Section	Presentation Mode [1]	Main Justification	Indicative Links
13.	Part II of the questionnaire	2.2.1. Phase I: Plan and Create	Tables 3 and 4	To address Objectives 3, 5, and 9	Section 2.1: Table 1 Section 2.2.1: Table 7 Section 2.2.3: Figures 5 and 6, Equation (1) Section 3: Figure 7 Section 3.1.2: Figures 12–14 Section 3.2.2: Figure 18 Section 3.2.3: Figure 21
14.	Survey design	2.2.1. Phase I: Plan and Create	Tables 5–7	To address Objectives 1, 6, 7, and 9	Sections 2.2 and 3
15.	Survey analysis plan	2.2.1. Phase I: Plan and Create	Table 7	To address Objective 8	Section 1 Section 2.2.1: Tables 2–4 Section 2.2.3: Figures 5 and 6, Equations (1)–(4) Section 3
16.	Target survey respondents	2.2.2. Phase II: Launch and Run	Text only	To address Objectives 1, 2, 4, 10, and 11	Section 2.2.1: Tables 2 and 7 Section 2.2.3: Figure 4, Step III.3 Section 3.1: Table 8 Section 3.1.1: Figure 8 Section 3.2.1: Figure 15 Section 3.2.3: Figure 19
17.	Analysis of survey responses	2.2.3. Phase III: Analyze and Report	Figure 5, Equations (1)–(4)	To address Objective 12	Section 1 Section 2.2.1: Tables 2–4 and Table 8 Section 2.2.3: Step III.3 Section 3
18.	Naming convention for identifying surveyed organizations	2.2.3. Phase III: Analyze and Report	Bullet points	To enhance the readability of Figure 14	Section 3.1.2: Figure 14
19.	Reporting of survey results	2.2.3. Phase III: Analyze and Report	Figure 6	To address Objective 12	Section 2.2.1: Tables 2–4 and Table 8 Section 2.2.3: Step III.2 Section 3
20.	Survey results	3. Results	Figure 7	To address Objectives 1 and 12	Section 1, Section 2, and Section 5
21.	Results for all surveyed organizations	3.1. Results for Surveyed Large and Small-Medium Organizations	Table 8, Figures 8–14	To address Objectives 1 and 12	Sections 1, 2, 3.2, 4 and 5
22.	Results for surveyed large organizations	3.2. Results for Surveyed Large Organizations	Figures 15–18	To address Objectives 1 and 12	Sections 1, 2, 3.1, 4 and 5

Table A1. *Cont.*

No.	Possible Item of Interest	Our Mapping			
		Section	Presentation Mode [1]	Main Justification	Indicative Links
23.	Results for surveyed large TMT organizations	3.2.3. Results for Surveyed Large Organizations from Technology, Media, & Telecom (TMT)	Figures 19–21	To address Objectives 1 and 12	Sections 1, 2, 3.1, 3.2.1, 3.2.2, 4 and 5
24.	Related works	4. Related Work	Tables 9 and 10	To compare our research with related works	Sections 1, 2.2, 3 and 5
25.	Conclusions and future work	5. Conclusions and Future Work	Text only	To summarize our work and point out future work	Sections 1–4

[1] Note the "Presentation Mode" for the possible item of interest is indicated through bullet points, text only, or specific figures, tables, and/or equations, where "Text only" indicates that the possible item of interest is outlined only using text.

Appendix B

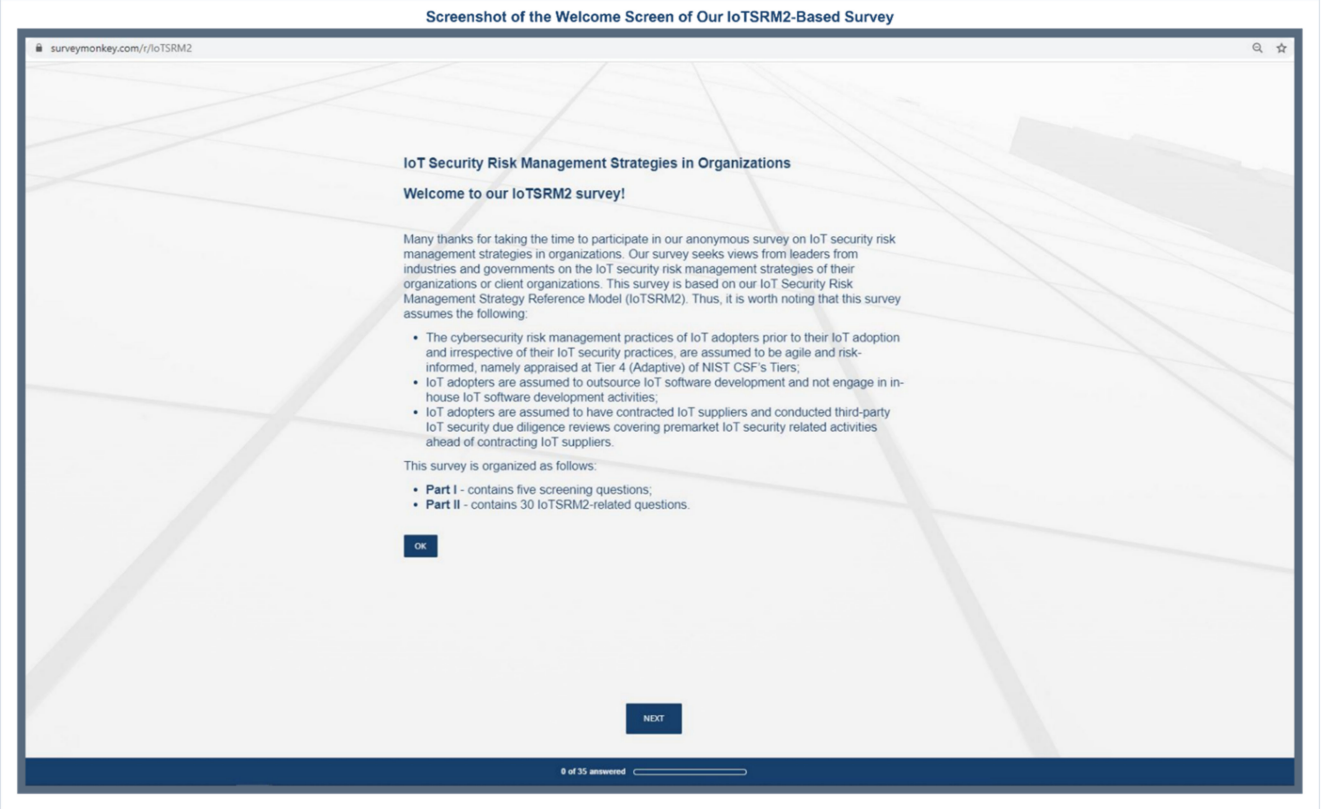

Figure A1. Screenshot of the welcome screen of our IoTSRM2-based survey.

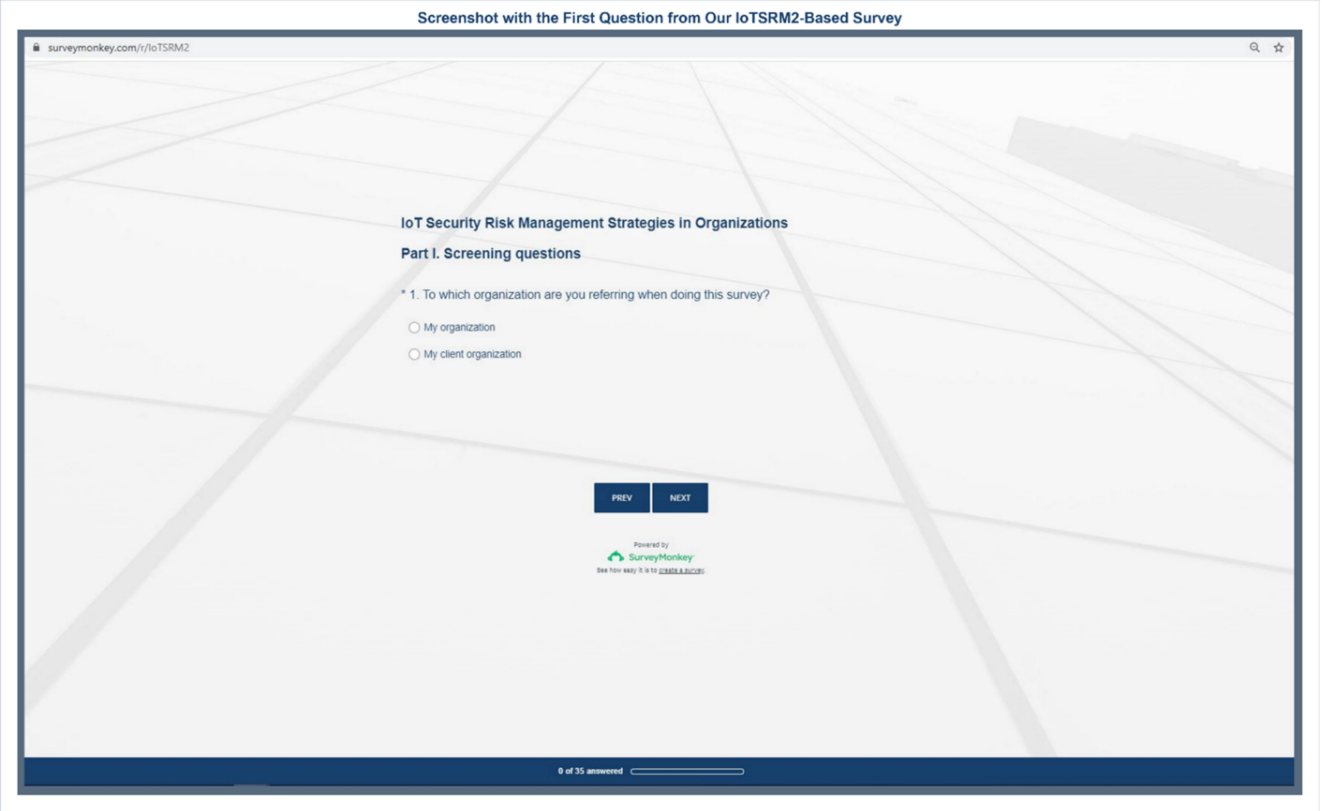

Figure A2. Screenshot with the first question from our IoTSRM2-based survey.

Appendix C

Table A2. Summary of the survey responses in numbers per IoTSRM2 controls and related questions.

IoTSRM2 Question ID	IoTSRM2 Control	No. of "No, to a Great Extent"	No. of "No, to a Certain Extent"	No. of "Yes, to a Certain Extent"	No. of "Yes, to a Great Extent"
6	IoT hardware assets inventory	6	12	10	3
7	IoT software assets inventory	8	11	11	1
8	Criticality and impact analysis	5	12	13	1
9	Resiliency requirements	5	5	15	6
10	IoT security policy	5	9	13	4
11	Privacy policy	7	7	16	1
12	Vulnerability disclosure policy	7	9	12	3
13	End-of-Life policy	7	12	11	1
14	IoT security governance structures and responsibilities	5	9	12	5
15	IoT security operations roles and responsibilities	5	6	14	6
16	Cybersecurity regulatory framework	6	7	13	5
17	IoT security and privacy controls management plan	5	11	12	3
18	IoT security budget plan	6	10	11	4

Table A2. *Cont.*

IoTSRM2 Question ID	IoTSRM2 Control	No. of "No, to a Great Extent"	No. of "No, to a Certain Extent"	No. of "Yes, to a Certain Extent"	No. of "Yes, to a Great Extent"
19	IoT security measurement and reporting plan	8	10	11	2
20	IoT security training and awareness plan	8	13	9	1
21	IoT security incident response plan	7	9	10	5
22	IoT vulnerability management plan	5	8	14	4
23	IoT End-of-Life plan	7	14	8	2
24	Disclosure-based IoT vulnerability discovery	6	7	12	6
25	Assessment-based IoT vulnerability discovery	5	8	14	4
26	Intelligence-driven IoT threat identification	6	9	11	5
27	Assessment-based IoT threat identification	7	9	11	4
28	IoT risk identification and analysis	5	7	15	4
29	Cybersecurity risk register and IoT risk responses	5	8	14	4
30	IoT security risk appetite and tolerances	5	15	6	5
31	Context-informed IoT security risk tolerances	4	14	8	5
32	IoT supply chain risk management plan	6	13	9	3
33	IoT supply chain risk assessment	7	13	9	2
34	IoT supplier contract management plan	10	10	9	2
35	IoT trustworthiness requirements	10	7	11	3

References

1. Giuca, O.; Popescu, T.M.; Popescu, A.M.; Prostean, G.; Popescu, D.E. A Survey of Cybersecurity Risk Management Frameworks. In *Soft Computing Applications. SOFA 2018. Advances in Intelligent Systems and Computing*; Balas, V., Jain, L., Balas, M., Shahbazova, S., Eds.; Springer: Cham, Switzerland, 2021; Volume 1221, pp. 240–272. ISBN 978-3-030-51991-9.
2. World Economic Forum. *The Global Risks Report 2021*, 16th ed.; Insight Report; World Economic Forum: Geneva, Switzerland, 2021; Available online: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (accessed on 9 June 2021).
3. World Economic Forum. *Future Series: Cybersecurity, Emerging Technology and Systemic Risk*; Insight Report; World Economic Forum: Geneva, Switzerland, 2021; Available online: http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf (accessed on 9 June 2021).
4. Singh, R.P.; Javaid, M.; Haleem, A.; Suman, R. Internet of things (IoT) applications to fight against COVID-19 pandemic. *Diabetes Metab. Syndr. Clin. Res. Rev.* **2020**, *14*, 521–524. [CrossRef] [PubMed]
5. Kashani, M.H.; Madanipour, M.; Nikravan, M.; Asghari, P.; Mahdipour, E. A systematic review of IoT in healthcare: Applications, techniques, and trends. *J. Netw. Comput. Appl.* **2021**, *192*, 103164. [CrossRef]
6. Khanna, A.; Kaur, S. Internet of Things (IoT), applications and challenges: A comprehensive review. *Wirel. Pers. Commun.* **2020**, *114*, 1687–1762. [CrossRef]
7. Hassan, R.; Qamar, F.; Hasan, M.K.; Aman, A.H.M.; Ahmed, A.S. Internet of Things and Its Applications: A Comprehensive Survey. *Symmetry* **2020**, *12*, 1674. [CrossRef]

8. Gayialis, S.P.; Konstantakopoulos, G.D.; Kechagias, E.P.; Papadopoulos, G.A.; Ponis, S.T. Developing an advanced cloud-based vehicle routing and scheduling system for urban freight transportation. In *Advances in Production Management Systems. Smart Manufacturing for Industry 4.0*; Moon, I., Lee, G., Park, J., Kiritsis, D., Von Cieminski, G., Eds.; Springer: Cham, Switzerland, 2018; Volume 536, pp. 190–197.
9. Gayialis, S.P.; Konstantakopoulos, G.D.; Kechagias, E.P.; Papadopoulos, G.A. An Advanced Transportation System Based on Internet of Things. In Proceedings of the 10th Annual International Conference on Industrial Engineering and Operations Management (IEOM 2020), Dubai, United Arab Emirates, 10–12 March 2020; pp. 3007–3012, ISSN: 2169-8767. ISBN 978-1-5323-5952-1.
10. Kechagias, E.P.; Gayialis, S.P.; Konstantakopoulos, G.D.; Papadopoulos, G.A. An Application of an Urban Freight Transportation System for Reduced Environmental Emissions. *Systems* **2020**, *8*, 49. [CrossRef]
11. World Economic Forum. *State of the Connected World*, 2020 ed.; Insight Report; World Economic Forum: Geneva, Switzerland, 2020; Available online: http://www3.weforum.org/docs/WEF_The_State_of_the_Connected_World_2020.pdf (accessed on 9 June 2021).
12. Popescu, T.M.; Popescu, A.M.; Prostean, G.; Popescu, D.E. Cybersecurity Threat Rating Method Based on Potential Cyber Harm. In Proceedings of the 34th International Business Information Management Association Conference (IBIMA). Vision 2025: Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage, Madrid, Spain, 13–14 November 2019; Soliman, K.S., Ed.; pp. 5909–5920, ISBN 978-0-9998551-3-3.
13. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.C.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur.* **2021**, *105*, 102248. [CrossRef]
14. Popescu, T.M.; Popescu, A.M.; Prostean, G. IoT Security Risk Management Strategy Reference Model (IoTSRM2). *Future Internet* **2021**, *13*, 148. [CrossRef]
15. Palo Alto Networks. 2020 Unit 42 IoT Threat Report. Available online: https://start.paloaltonetworks.com/unit-42-iot-threat-report (accessed on 7 June 2021).
16. Popescu, T.M.; Popescu, A.M.; Prostean, G.; Popescu, D.E. Evaluation of legislations from the perspective of organizational understanding to managing cybersecurity risk. In Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020, Granada, Spain, 10–11 April 2019; Soliman, K.S., Ed.; pp. 4677–4689, ISBN 978-0-9998551-2-6.
17. US Congress. H.R.1668—Internet of Things Cybersecurity Improvement Act of 2020. Available online: https://www.congress.gov/bill/116th-congress/house-bill/1668/text (accessed on 8 June 2021).
18. DCMS. New Cyber Security Laws to Protect Smart Devices amid Pandemic Sales Surge. Available online: https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge (accessed on 8 June 2021).
19. Ponemon Institute. A New Roadmap for Third Party IoT Risk Management the Critical Need to Elevate Accountability, Authority and Engagement. Available online: https://sharedassessments.org/blog/a-new-roadmap-for-third-party-iot-risk-management/ (accessed on 9 June 2021).
20. Dillman, D.A.; Tortora, R.; Bowker, D. *Principles for Constructing Web Surveys*; Washington State University, Social and Economic Sciences Research Center: Pullman, WA, USA, 1999.
21. NIST. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed on 6 June 2021).
22. European Commission. SME Definition. Available online: https://ec.europa.eu/growth/smes/sme-definition_en (accessed on 12 June 2021).
23. Reyna, J.; Hanham, J.; Vlachopoulos, P.; Meier, P. Using factor analysis to validate a questionnaire to explore self-regulation in learner-generated digital media (LGDM) assignments in science education. *Australas. J. Educ. Technol.* **2019**, *35*, 128–152. [CrossRef]
24. Momentive. How to Create a Survey. Available online: https://help.surveymonkey.com/articles/en_US/kb/How-to-create-a-survey (accessed on 9 June 2021).
25. Irwin, C.W.; Stafford, E.T. *Survey Methods for Educators: Collaborative Survey Development*; Part 1 of 3; REL 2016–163; US Department of Education, Institute of Education Sciences, National Center for Education Evaluation and Regional Assistance, Regional Educational Laboratory Northeast & Islands: Washington, DC, USA, 2016.
26. Frippiat, D.; Marquis, N. Web Surveys in the Social Sciences: An Overview. *Population* **2010**, *65*, 285–311. [CrossRef]
27. Keusch, F. Why do people participate in Web surveys? Applying survey participation theory to Internet survey data collection. *Manag. Rev. Q.* **2015**, *65*, 183–216. [CrossRef]
28. Poon, P.S.; Albaum, G.; Evangelista, F.U. Why People Respond to Surveys. *J. Int. Consum. Mark.* **2004**, *16*, 75–90. [CrossRef]
29. Sánchez-Fernández, J.; Muñoz-Leiva, F.; Montoro-Ríos, F.J. Improving retention rate and response quality in Web-based surveys. *Comput. Hum. Behav.* **2012**, *28*, 507–514. [CrossRef]
30. Combs, J.P.; Onwuegbuzie, A.J. Describing and illustrating data analysis in mixed research. *Int. J. Educ.* **2010**, *2*, 1–23. [CrossRef]
31. Almutairi, O.; Almarhabi, K. Investigation of Smart Home Security and Privacy: Consumer Perception in Saudi Arabia. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 614–622. [CrossRef]
32. Arm Limited. Bridging the Gap PSA Certified Security Report 2021. How Collaboration will Secure the Future of IoT. Available online: https://report.psacertified.org/ (accessed on 7 June 2021).

33. Asplund, M.; Nadjm-Tehrani, S. Attitudes and Perceptions of IoT Security in Critical Societal Services. *IEEE Access* **2016**, *4*, 2130–2138. [CrossRef]
34. Cabinet Office. Consumer Attitudes Towards IoT Security. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978685/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf (accessed on 7 June 2021).
35. Forescout Technologies. The Enterprise of Things Security Report The State of IoT Security. Available online: https://www.forescout.com/the-enterprise-of-things-security-report-state-of-iot-security-in-2020/ (accessed on 7 June 2021).
36. Gemalto. The State of IoT Security. Available online: https://www.infopoint-security.de/media/gemalto-state-of-iot-security-report.pdf (accessed on 7 June 2021).
37. IBM. Electronics Industrial IoT Cybersecurity. Available online: https://www.ibm.com/thought-leadership/institute-business-value/report/electronicsiiot (accessed on 7 June 2021).
38. Juniper Networks. Securing IoT at Scale Requires a Holistic Approach Survey Insights Revealed by IoT Adopters. Available online: https://www.juniper.net/assets/kr/kr/local/pdf/ebooks/7400082-en.pdf (accessed on 7 June 2021).
39. SANS Institute. The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns. Available online: https://www.forescout.com/2018-sans-industrial-iot-security-survey/ (accessed on 7 June 2021).
40. UL. Security Concerns Escalate as IoT Expands Market Insights on the State of IoT Security. Available online: https://www.ul.com/sites/g/files/qbfpbp251/files/2019-04/security-concerns-escalate-as-iot-expands.pdf (accessed on 7 June 2021).