future internet

MDPI

Article

IoT Security Risk Management Strategy Reference Model (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@mpt.upt.ro
[2] PactFlux SRL, 101, Leurda, 215204 Motru, Romania; pampopescu2017@gmail.com
* Correspondence: traian.popescu@student.upt.ro

Abstract: Nowadays, Internet of Things (IoT) adoptions are burgeoning and deemed the lynchpin towards achieving ubiquitous connectivity. In this context, defining and leveraging robust IoT security risk management strategies are paramount for secure IoT adoptions. Thus, this study aims to support IoT adopters from any sector to formulate or reframe their IoT security risk management strategies to achieve robust strategies that effectively address IoT security issues. In a nutshell, this article relies on a mixed methods research methodology and proposes a reference model for IoT security risk management strategy. The proposed IoT security risk management strategy reference model (IoTSRM2) relies on the 25 selected IoT security best practices which are outlined using a proposed taxonomic hierarchy, and on the proposed three-phased methodology that consists of nine steps and outputs. The main contribution of this work is the proposed IoTSRM2 which consists of six domains, 16 objectives, and 30 prioritized controls. Furthermore, prior to providing the related work, this article provides a critical evaluation of selected informative references of IoTSRM2 based on their percentage-wise linkage to the IoTSRM2 domains and to the entire IoTSRM2. The findings of the critical evaluation illustrate, inter alia, the selected informative references that are the top three most and least linked to the entire IoTSRM2.

Keywords: Internet of Things; IoT security; cybersecurity; risk management; strategy; reference model; standards; guidelines; frameworks; best practices

check for updates

Citation: Popescu, T.M.; Popescu, A.M.; Prostean, G. IoT Security Risk Management Strategy Reference Model (IoTSRM2). *Future Internet* **2021**, *13*, 148. https://doi.org/10.3390/fi13060148

Academic Editor: Weizhi Meng

Received: 12 May 2021
Accepted: 31 May 2021
Published: 4 June 2021

1. Introduction

Today, cybersecurity spending is primarily driven by the need to face the proliferation of cyber threats [1], the fear of non-compliance with domestic and cross-border cybersecurity regulations [2], and the want to embark on the digitalization rush at the cost of wider attack surface [3]. These key drivers are also highlighted in the studies conducted by Giuca et al. [4] and the Ponemon Institute [5]. In other words, opportunity-driven organizations everywhere strive to keep pace with or even dominate the digital transformation (DX) race in an increasingly digitally connected world where cyber risks are thriving and cybersecurity regulations are getting tougher [4,6]. According to A.T. Kearney's "Views from the C-Suite" survey, although the leading operational challenges faced by organizations are the rising cybersecurity risks and the difficulty in adopting new technologies, the top operations opportunity for organizations is the successful adoption of new technologies [6].

Moreover, in the context of operating in the digital world of fast-paced innovation, connectivity, and real-time information, the worldwide adoption of Internet of Things (IoT) technologies is burgeoning, and its associated economic impact is substantial and expected to keep growing in the coming years. Various reports from organizations and academia underscored these aspects by either stating these facts or providing different projections which present significant variability based on their approach, base year, and forecast period. For instance, the Ponemon Institute [5] surveyed 630 individuals on third party IoT risk management and their survey report revealed, among others, that the number of connected IoT devices is expected to double within the next two years. As part of the AT&T cybersecurity insights report, AT&T [7] pointed out the rapid growth of connected IoT devices worldwide which resulted from the 500 individuals surveyed on the state of IoT security. As part of the Congressional Research Service (CRS) report on IoT, CRS [8] reported the forecast of the market research firm IoT Analytics which predicted that the number of global active IoT devices will substantially rise from 9.9 billion in 2019 to 21.5 billion in 2025 and that the global IoT market growth is expected to reach USD 1.56 billion by 2025. According to Deloitte's report on IoT, the global IoT spending is projected to grow from USD 726 billion in 2019 to USD 1.1 trillion by 2023 [9]. As highlighted by the International Electrotechnical Commission (IEC) [10], IoT has a significant impact on the global economy based on the IoT market forecasts of three worldwide well-renowned consulting firms. As part of the Juniper Research's whitepaper on IoT, Juniper Research [11] provided a more aggressive projection for the total global number of IoT connections which could get to 83 billion by 2024. According to Lee [12], an increasing number of IoT devices are connected. This increasing tendency of organizations to connect more and more devices, products, and systems is also articulated as part of the McKinsey & Company's insights report, where McKinsey & Company [13] indicated this tendency as a key driver towards the massive rise of IoT. McKinsey & Company [14] also anticipated a steady growth of IoT investments and the increase of the worldwide number of IoT connected devices to 43 billion by 2023. The prospects of IoT growth were echoed by World Economic Forum [15] which predicted 25 billion connected IoT devices globally by 2025. As part of another insight report, World Economic Forum [16] increased their expectation from 25 billion connected devices worldwide to 41.6 billion and highlighted the investment growth surrounding IoT adoption.

Furthermore, IoT adoption will soar with the deployment of the 5G technology as it enables much more connected devices to benefit from far better mobile communications. For example, CRS [8] pointed out that the deployment of 5G cellular networks and technologies will drive IoT growth. Juniper Research [11] adopted a similar tone on the IoT growth indicating 5G as a key driver for IoT adoption. With respect to the perks of leveraging 5G technology, the World Economic Forum [15] indicated 5G as a core component of IoT as it enables greater speeds and reliability of communications for much more IoT devices. According to McKinsey & Company's insights report, McKinsey & Company [17] highlighted that the revenues for 5G IoT modules and components will rise over time, which implicitly links the growth of IoT adoption to 5G deployment.

It is worth noting that IoT denotes a system of interconnected homogeneous and/or heterogeneous systems and services that enable information processing and various interactions. This definition of IoT is derived from and based on the definitions from the CRS [8], IEC [10], and Garcia-Morchon et al. [18]. In this sense, it is safe to say that IoT is fundamental towards achieving ubiquitous connectivity in this era of digital transformation [15,19,20].

Notwithstanding, for IoT, the current state of risk management is far behind the target state. Hence, the Ponemon Institute [5] underlined the burning need to place IoT risk management improvement high on the agenda. A.T. Kearney [6] placed poorer practices in risk management among the top ten business operations' challenges following their survey of around 450 senior executives of the world's leading organizations. As part of Deloitte's report on IoT, Deloitte [9] reported the finding of the Open Web Application Security Project (OWASP), which indicated the absence of integrated risk management approach for IoT data lifecycle management as a widespread challenge. World Economic Forum [16] pointed out immature IoT risk management capabilities, which may lead to poor IoT risk management practices. According to Bain [21], the majority of the 280 executives surveyed indicated a great level of concern around the IoT risks to which their organizations are exposed.

In the context of managing IoT risk, cybersecurity related issues give rise to the greatest level of concern, and cybersecurity is regarded as pivotal for organizations. For instance, IEC [10] named security, trust, privacy, and identity management among the key limitations and deficiencies of today's IoT. As part of the World Economic Forum's report on the global state of IoT, World Economic Forum [16] highlighted privacy and trust, and safety and security as the top risk impact areas of IoT governance for organizations, which resulted from the 374 global IoT stakeholders surveyed. The great concern around cybersecurity is also reflected in the findings from the survey conducted by McKinsey & Company, where cybersecurity resulted in being the top priority for organizations when acquiring IoT products based on the responses from 1161 global IoT practitioners [22]. As part of the AT&T cybersecurity insights report, AT&T [7] claimed that IoT security is the top concern of the Chief Executive Officer's (CEO) agenda. According to findings from the study conducted by McKinsey & Company [13], 75% of the 400 IoT experts surveyed indicated IoT security as either important or very important. As per the findings of Bain [21], the more mature are the organizations in terms of their cybersecurity capabilities, the more importance they place on their IoT risks.

Hence, IoT security risk management may raise the greatest level of concern among organizations as there is no general IoT security model [10], there is no global IoT security standard [16], there are only a few IoT security standards [13], and most best practices are not focused on IoT security risk management [12,15]. Moreover, cybersecurity strategies tend to be developed reactively rather than proactively in the transformation journey [3,16,23]. In this context, it is very likely that, amid adopting IoT, many organizations out there lack adequate IoT security risk management strategies. For instance, Lee [12] highlighted the findings of a recent survey that revealed that very few of the survey participants had a cybersecurity strategy in place that incorporates IoT security requirements. The lack of cybersecurity strategies that cover IoT was also pointed out by McKinsey & Company for a fairly considerable number of organizations [13].

Considering this prevalent absence of robust IoT security risk management strategies in organizations coupled with the paucity of IoT security risk management strategy reference sources, there is a clear research gap in terms of the existence of an IoT security risk management strategy reference model. Thus, the purpose of this research article is to propose an IoT security risk management strategy reference model (IoTSRM2) that aims to support practitioners from organizations embracing IoT technologies to formulate or reframe their IoT security risk management strategies and achieve secure IoT adoption. Moreover, the proposed IoTSRM2 aims to support fellow researchers from academia that seek to explore the topic of IoT security risk management strategy as part of their research works. To address the aforementioned research gap and achieve the desired IoTSRM2, this article relies on a mixed methods research methodology harnessing both qualitative and quantitative methods. Hence, this research work makes use of quantitative data to complement the qualitative data, which adds value to the outputs of this research and allows the proposed IoTSRM2 to become more actionable through a means for prioritization of IoTSRM2 controls. In this context, the outputs of this research work concretize into the main contributions outlined below:

- The development of a taxonomic hierarchy for classifying IoT security best practices based on their applicability to specific groups of target audience and type of IoT security best practice;
- The identification of some of the most well-renowned IoT security best practices, the classification of these best practices based on the proposed taxonomic hierarchy, and the summarization of these best practices;
- The design of a methodology for developing the IoT security risk management strategy reference model;
- The development of a reference model for IoT security risk management strategy based on best practices that is suitable for IoT adopters from any sector;

- A critical evaluation of some of the IoT security best practices based on their linkage to the proposed reference model;
- A comparative analysis of the related work for the proposed reference model based on a set of evaluation criteria.

Beyond this introductory section, the remainder of this article is organized as follows. Section 2 provides an overview of IoT security best practices and describes the three-phased methodology for developing the proposed IoT security risk management strategy reference model (IoTSRM2). Section 3 first presents the proposed IoTSRM2 including the IoTSRM2 domains, objectives, and controls, the informative references for each IoTSRM2 control, and the prioritization of IoTSRM2 controls for each IoTSRM2 objective. Then, Section 3 provides the critical evaluation of selected informative references of IoTSRM2. Section 4 presents the related work. Finally, Section 5 presents the concluding remarks and future work.

2. Materials and Methods

This section is structured in two subsections. Section 2.1 gives an overview of IoT security best practices. First, it provides the rationale behind selecting the IoT security best practices and enumerates the 25 selected IoT security best practices. Second, it proposes a novel taxonomic hierarchy for classifying the selected IoT security best practices. Third, it gives the overview of IoT security best practices using our proposed taxonomic hierarchy. Afterwards, Section 2.2 describes our three-phased methodology for developing the proposed IoTSRM2.

2.1. Overview of IoT Security Best Practices

There are numerous best practices in the literature relevant to IoT security. Although this overview does not provide an exhaustive list of IoT security best practices, it focuses on some of the most renowned best practices which are relevant to IoT security irrespective of their target audience, are applicable vertically or horizontally across sectors, and are available in English. In this context, the identification of the in-scope IoT security best practices is based on the current state of the art (i.e., [18,24]), available mappings of IoT security recommendations, guidance, and standards to IoT security best practices (i.e., [25–29]), and references to IoT security best practices from other research works (i.e., [30,31]). This identification is also based on online searches of IoT security initiatives from the Cloud Security Alliance (CSA), the European Union Agency for Cybersecurity (ENISA), and the National Institute of Standards and Technology (NIST). With respect to exclusions, this overview does not cover exclusively technically-focused IoT security best practices or IoT security best practices which are intended for the purpose of certification. Moreover, this overview focuses on final versions of IoT security best practices and does not cover draft or expired ones. Furthermore, it does not cover cybersecurity best practices that are not IoT security specific, and it does not capture vendor reports that address IoT security best practices. Therefore, the main categories of IoT security best practices that are considered beyond the scope of this overview are listed below along with a few notable examples of best practices:

- **Exclusively technically-focused IoT security best practices**, such as:
  - ○ Concise Binary Object Representation (CBOR) Object Signing and Encryption (COSE) published by Internet Engineering Task Force (IETF) [32]
- **IoT security best practices intended for the purpose of certification**, such as:
  - ○ CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.2.2 issued by CTIA Certification [33]
  - ○ PSA Certified™ Level 1 Questionnaire, Version 2.1 published by Platform Security Architecture (PSA) Joint Stakeholder Agreement (JSA) Members [34]
- **Draft IoT security best practices**, such as:
  - ○ oneM2M TR-0008-V2.0.1 Security (Technical Report) issued by oneM2M Partners [35]

- **Expired IoT security best practices**, such as:
  - ○ Best Current Practices for Securing Internet of Things (IoT) Devices [36]
- Cybersecurity best practices that are not IoT security specific, such as:
  - ○ The Open Web Application Security Project (OWASP) Secure Coding Practices Quick Reference Guide [37]
  - ○ Fundamental Practices for Secure Software Development 2nd Edition A Guide to the Most Effective Secure Development Practices in Use Today published by Software Assurance Forum for Excellence in Code (SAFECode) [38]
  - ○ Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure System published by National Institute of Standards and Technology (NIST) [39]
- **Vendor reports covering IoT security best practices**, such as:
  - ○ AT&T Cybersecurity Insights: The CEO's Guide to Securing the Internet of Things [7]

Thus, Table 1 illustrates the 25 selected IoT security best practices, and outlines for each best practice its corresponding publisher and reference.

Table 1. Selected IoT security best practices.

Publisher	Name	Reference
AgeLight LLC	IoT Safety Architecture and Risk Toolkit v4.0	[40]
Alliance for Internet of Things Innovation (AIOTI)	Report on Workshop on Security and Privacy in the Hyper-Connected World	[41]
Australian Government	Code of Practice Securing the Internet of Things for Consumers	[42]
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	[43]
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	[44]
Cloud Security Alliance (CSA)	Identity and Access Management for the Internet of Things—Summary Guidance	[45]
Cloud Security Alliance (CSA)	CSA IoT Security Controls Framework Version 1	[46]
Council to Secure the Digital Economy (CSDE)	The C2 Consensus on IoT Device Security Baseline Capabilities	[26]
European Telecommunications Standards Institute (ETSI)	ETSI European Standard (EN) 303.645 V2.1.1 Cyber Security for Consumer Internet of Things: Baseline Requirements	[30]
GSM Association (GSMA)	GSMA IoT Security Assessment Checklist Version 3.0	[47]
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework	[48]
Institute of Electrical and Electronics Engineers (IEEE)	Internet of Things (IoT) Security Best Practices	[49]
IoT Security Foundation (IoTSF)	IoT Security Compliance Framework Release 2.1	[50]
Japan's IoT Acceleration Consortium (IoTAC)	IoT Security Guidelines Ver. 1.0	[51]
National Electrical Manufacturers Association (NEMA)	Cyber Hygiene Best Practices	[52]
National Institute of Standards and Technology (NIST)	Foundational Cybersecurity Activities for IoT Device Manufacturers	[53]
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	[54]

Table 1. *Cont.*

Publisher	Name	Reference
The European Union Agency for Cybersecurity (ENISA)	Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures	[28]
The European Union Agency for Cybersecurity (ENISA)	Good Practices for Security of Internet of Things in the context of Smart Manufacturing	[55]
The European Union Agency for Cybersecurity (ENISA)	Good Practices for Security of IoT Secure Software Development Lifecycle	[56]
The European Union Agency for Cybersecurity (ENISA)	Procurement Guidelines for Cybersecurity in Hospitals Good practices for the security of Healthcare services	[57]
The European Union Agency for Cybersecurity (ENISA)	Guidelines for Securing the Internet of Things Secure supply chain for IoT	[58]
U.S. Department of Homeland Security (DHS)	Strategic Principles for Securing the Internet of Things (IoT) Version 1.0	[59]
U.S. Department of Transportation National Highway Traffic Safety Administration (NHTSA)	Cybersecurity Best Practices for Modern Vehicles	[60]
United Kingdom Department for Digital, Culture, Media and Sport (UK DCMS)	Code of Practice for Consumer IoT Security	[61]

Furthermore, Figure 1 illustrates our proposed taxonomic hierarchy for classifying the 25 selected IoT security best practices, which emerged from the review of these IoT security best practices. Our taxonomic hierarchy aims to classify the selected best practices based on their applicability to specific groups of target audience and type of IoT security best practice. Thus, the selected IoT security best practices are grouped into the four categories below based on their applicability to specific groups of target audience:

- **Adopter specific:** this category denotes IoT security best practices that are applicable primarily to IoT adopters;
- **General**: this category denotes IoT security best practices that are applicable to IoT adopters, IoT manufacturers, and/or IoT suppliers;
- **Manufacturer specific:** this category denotes IoT security best practices that are applicable primarily to IoT manufacturers;
- **Supplier specific:** this category denotes IoT security best practices that are applicable primarily to IoT suppliers.

As for the next level of the taxonomic hierarchy, the selected IoT security best practices are grouped into the four categories below based on their corresponding type:

- **Codes of practice:** this category denotes IoT security voluntary principles [42] or guidelines [61] recommended by governments for industry as the minimum standard for a specific topic [42], which do not take precedence over national legislation in any country [62];
- **Standards:** this category denotes agreed IoT security best practices developed by external standards organizations which consist of requirements, specifications, guidelines, or characteristics for activities or for their outputs, that are generally complied with for making a product, managing a process, delivering a service, or supplying materials [4];
- **Guidelines:** this category denotes IoT security recommendations on how something should be done for achieving an objective [63], and these recommendations are less prescriptive than procedures [64];
- **Frameworks:** this category denotes logical structures or models that rely on a set of guiding principles, may not get into the detailed processes and procedures, may refer to a collection of standards and best practices (e.g., methodologies, methods, etc.) that underpin their underlying principles, and are aimed at enabling IoT security programs [4].

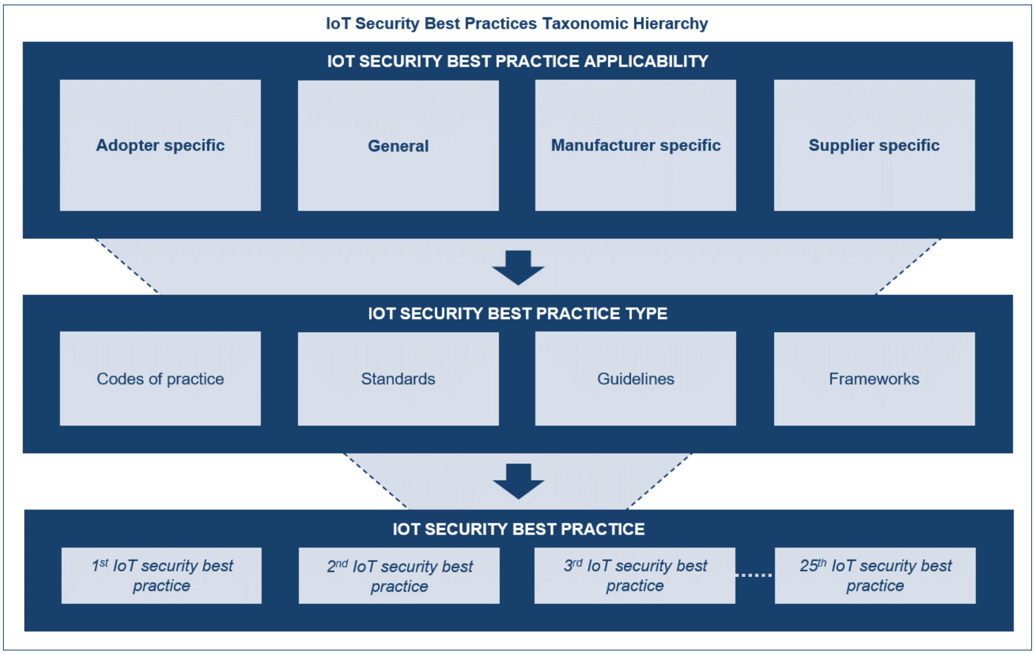
IoT Security Best Practices Taxonomic Hierarchy
IOT SECURITY BEST PRACTICE APPLICABILITY
Adopter specific
General
Manufacturer specific
Supplier specific
IOT SECURITY BEST PRACTICE TYPE
Codes of practice
Standards
Guidelines
Frameworks
IOT SECURITY BEST PRACTICE
1st IoT security best practice
2nd IoT security best practice
3rd IoT security best practice
25th IoT security best practice

Figure 1. Our proposed taxonomic hierarchy for IoT security best practices.

Furthermore, Table 2 shows the references of the reviewed IoT security best practices mapped against the corresponding categories of IoT security best practices from the proposed taxonomic hierarchy.

Furthermore, an overview of these IoT security best practices is provided under individual subsubsections that correspond to the four categories of IoT security best practices based on their applicability to specific groups of target audience. As part of each subsubsection, the corresponding IoT security best practices are outlined under their corresponding category based on the type of IoT security best practice.

Table 2. Selected IoT security best practices with their taxonomic categories.

Applicability	Type	IoT Security Best Practice	Reference
Adopter specific	Guidelines	CSA's Security Guidance for Early Adopters of the Internet of Things (IoT)	[44]
		CSA's Identity and Access Management for the Internet of Things—Summary Guidance	[45]
		ENISA's Procurement Guidelines for Cybersecurity in Hospitals Good practices for the security of Healthcare services	[57]
	Frameworks	CSA IoT Security Controls Framework Version 1	[46]
General	Codes of practice	U.S. DHS's Strategic Principles for Securing the Internet of Things (IoT) Version 1.0	[59]
		Japan's IoTAC IoT Security Guidelines Ver. 1.0	[51]
	Guidelines	ENISA's Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures	[28]
		ENISA's Good Practices for Security of Internet of Things in the context of Smart Manufacturing	[55]
		ENISA's Good Practices for Security of IoT Secure Software Development Lifecycle	[56]
		ENISA's Guidelines for Securing the Internet of Things Secure supply chain for IoT	[58]
	Frameworks	AgeLight's IoT Safety Architecture & Risk Toolkit v4.0	[40]
		IIC's Industrial Internet of Things Volume G4: Security Framework	[48]
		OTA's IoT Security & Privacy Trust Framework v2.5	[54]

Table 2. *Cont.*

Applicability	Type	IoT Security Best Practice	Reference
Manufacturer specific	Standards	ETSI European Standard (EN) 303.645 V2.1.1 Cyber Security for Consumer Internet of Things: Baseline Requirements	[30]
		NEMA's Cyber Hygiene Best Practices	[52]
	Guidelines	BITAG's Internet of Things (IoT) Security and Privacy Recommendations	[43]
		CSDE's The C2 Consensus on IoT Device Security Baseline Capabilities	[26]
		IEEE's Internet of Things (IoT) Security Best Practices	[49]
		NIST's Foundational Cybersecurity Activities for IoT Device Manufacturers	[53]
Supplier specific	Codes of practice	UK DCMS's Code of Practice for Consumer IoT Security	[61]
		Australian Government's Code of Practice Securing the Internet of Things for Consumers	[42]
	Guidelines	AIOTI's Report on Workshop on Security and Privacy in the Hyper-Connected World	[41]
		U.S. NHTSA's Cybersecurity Best Practices for Modern Vehicles	[60]
	Frameworks	GSMA's IoT Security Assessment Checklist Version 3.0	[47]
		IoTSF's IoT Security Compliance Framework Release 2.1	[50]

2.1.1. Adopter Specific IoT Security Best Practices

This subsubsection provides an overview of the selected IoT security best practices which are applicable only to IoT adopters, namely the adopter specific IoT security guidelines and the adopter specific IoT security framework.

Adopter Specific IoT Security Guidelines

The IoT security best practices below are guidelines that address generic-based IoT security controls [44], IoT recommendations specific to Identity and Access Management [45], or healthcare-specific IoT security good practices [57]. These selected guidelines are outlined below:

- **CSA's Security Guidance for Early Adopters of the Internet of Things (IoT):** Provides key challenges for secure IoT adoption and recommended security controls for IoT adopters to implement at different layers of the protocol stack [18]. The recommended controls are grouped into seven categories which focus on IoT privacy impact assessment and privacy-by-design, secure IoT systems engineering, layered security protections for IoT assets, data protection, security controls for IoT devices, authentication/authorization framework for IoT deployments, and logging and audit framework for IoT environment [44];
- **CSA's Identity and Access Management for the Internet of Things—Summary Guidance:** Extends the guidance on IoT Identity and Access Management (IAM) from [44]. It provides a set of IAM related recommendations to support IoT adopters [45];
- **ENISA's Procurement Guidelines for Cybersecurity in Hospitals Good practices for the security of Healthcare services:** This report focuses on providing cybersecurity guidelines to healthcare organizations for improving their procurement process of medical devices and applies to healthcare professionals including Chief Information Security Officers (CISOs), Chief Technology Officers (CTOs), IT teams, and procurement officers. First, the report provides cybersecurity considerations for planning, sourcing, and managing procured systems and services which are further grouped into ten procurement types. Then, it provides an overview of cybersecurity-related regulations, international standards, and good practices for healthcare systems, products, and services, and outlines the relevance of each of these best practices to the selected

procurement types. Furthermore, the report provides key cybersecurity challenges, a cyber threat taxonomy, and key procurement-related risks for hospitals. In addition, it provides a set of cybersecurity good practices for each procurement phase (i.e., plan, source and manage), which are then mapped against the procurement types and related threats [57].

Adopter Specific IoT Security Framework

The selected adopter specific IoT security framework is outlined below:

- **CSA IoT Security Controls Framework Version 1:** The framework applies to designers, developers, and evaluators for evaluating and implementing the enterprise IoT systems [65]. It provides 160 IoT security controls grouped into 26 categories. For each recommended control, it provides the following details: control specification, the reference to its corresponding control identification number from the CSA Cloud Controls Matrix (CCM), the IoT system risk impact levels (i.e., in terms of confidentiality, integrity, and availability), supplemental control guidance, implementation guidance, and its applicability to edge, fog, and cloud IoT system components. The framework is supplemented by a guide that provides instructions for using the framework. In addition, this framework's guide makes reference to two NIST publications (i.e., FIPS PUB 199 [66], FIPS PUB 200 [67]) which should support organizations to determine the risk impact level pertaining to their system's data prior to implementing the security controls from the proposed framework [46].

2.1.2. General IoT Security Best Practices

This subsubsection provides an overview of the selected IoT security best practices which are general in nature in terms of their applicability. Each of these best practices is outlined below under its corresponding type-based category (i.e., codes of practice, guidelines, frameworks).

General IoT Security Codes of Practice

The selected general IoT security codes of practice focus on secure IoT systems development lifecycle [51,59], and are outlined below:

- **U.S. DHS's Strategic Principles for Securing the Internet of Things (IoT) Version 1.0:** Provides six strategic non-binding principles with suggested practices for each principle to support secure IoT systems development lifecycle [59]. These principles focus on four categories of IoT stakeholders (i.e., IoT developers, IoT manufacturers, service providers, and industrial and business-level consumers) [59]. Garcia-Morchon et al. [18] describe this code of practice in a similar manner, and ECSO [24] also provides a concise description covering the focus of this code of practice;
- **Japan's IoTAC IoT Security Guidelines Ver. 1.0:** It is twofold: firstly, it outlines 21 key concepts spread across five guiding principles for IoT security measures, where each principle corresponds to one stage of the IoT systems development lifecycle (i.e., policy, analysis, design, implementation and connection, and operation and maintenance), and, secondly, it provides four IoT security recommendations to raise awareness among the general public on how to use IoT devices safely. In addition, it provides the mapping of target users (i.e., executives, IoT device manufacturers, system and service providers/corporate users) against key concepts, along with the mapping of general public to recommendations [51].

General IoT Security Guidelines

All reviewed general IoT security guidelines are published by ENISA. Two of these are applicable to sector-specific organizations [28,55], one guideline focuses on secure IoT systems development lifecycle [56], and another one focuses on secure IoT supply chain [58]. These general IoT security guidelines are outlined below:

- **ENISA's Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures:** This report focuses on critical information infrastructures (CII) and applies to IoT adopters, IoT manufacturers and operators, specific IT personnel profiles (e.g., IoT experts, IT/security solutions architects), and regulators. First, it provides an IoT high-level reference model, IoT asset, and threat taxonomies, and mapping of identified IoT threats against the IoT assets. Then, it provides a set of IoT security measures/good practices which are grouped into three categories (i.e., policies, organizational, people and process measures, and technical measures), to address the identified IoT threats, vulnerabilities, and risks. Furthermore, it provides an IoT security gap analysis and seven recommendations that aim to address the identified IoT security gaps. In addition, it provides references for each recommended security measure/good practice, mapping of security measures to threat groups, and the target audience for each of the seven recommendations [28];

- **ENISA's Good Practices for Security of Internet of Things in the Context of Smart Manufacturing:** This study focuses on Smart Manufacturing organizations and applies to operators, manufacturers, and users of Industrial Internet of Things (IIoT). First, it provides a high-level reference model for a smart manufacturing environment, asset and threat taxonomies for Industry 4.0, and mapping of the identified IIoT threats against IIoT assets. Then, it provides a set of security measures/good practices which are grouped into three categories (i.e., policies, organizational practices, and technical practices), to address the identified threats for IIoT environments. In addition, it provides references for each recommended security measure/good practice and for each threat group [55];
- **ENISA's Good Practices for Security of IoT Secure Software Development Lifecycle:** Provides guidelines for IoT software developers, IoT integrators, platform and system engineers, and consumers for securing the Software Development Lifecycle (SDLC) of IoT systems and services. First, it provides the key cybersecurity challenges and considerations for IoT SDLC by describing each SDLC phase (i.e., requirements analysis, software design, development/implementation, testing and acceptance, deployment and integration, and maintenance and disposal). Then, it provides asset and threat taxonomies related to the IoT SDLC along with the mapping of the identified threats against IoT assets. Furthermore, it provides a set of IoT SDLC related security measures which are grouped into three categories (i.e., people, processes, and technologies). In addition, it provides a table for each category of measures that captures the recommended security measures mapped against the identified threats, secure SDLC phases, and corresponding references [56];
- **ENISA's Guidelines for Securing the Internet of Things Secure Supply Chain for IoT:** This report provides guidelines for securing the IoT supply chain and applies to a wide range of profiles including IoT software developers and manufacturers, information security experts, IT/security solutions architects, Chief Information Security Officers (CISOs), Critical Information Infrastructure Protection (CIIP) experts, project managers, and procurement teams. First, it addresses the cybersecurity challenges related to each of the IoT supply chain stages (i.e., conceptual, development, production, utilization, support, and retirement), and it provides the related threats. Furthermore, it provides security good practices which are classified into three groups (i.e., actors, processes, and technologies). In addition, it includes references for each recommended security good practice and outlines the mapping of related threats and supply chain stages to good practices for each group of secure IoT supply chain good practices [58].

General IoT Security Frameworks

The selected general IoT security frameworks provide strategic IoT security principles [40,54] or trustworthiness requirements [48]. These frameworks are outlined below:

- **AgeLight's IoT Safety Architecture and Risk Toolkit v4.0:** Provides 44 principles which are grouped into four categories (i.e., security by design, user identity and authentication, privacy, disclosures and transparency, related safety, privacy and usability enhancing principles) and are mapped to some related best practices and regulations. It also provides rating values from "1" (i.e., low impact) to "10" (i.e., high impact) to be used by organizations for rating their risk (i.e., user benefit, ecosystem impact, financial impact, hazardization, development effort and costs, regulatory risk) while performing risk assessments against these recommended principles [40];

- **IIC's Industrial Internet of Things Volume G4: Security Framework**: This framework [48] provides business, functional, and implementation viewpoints for enabling trustworthy Industrial Internet of Things (IIoT) systems by explaining the ways to deal with security and privacy risks through technologies and processes. This framework is intended for a diverse audience spanning from IIoT owners to any stakeholder interested in security and trustworthiness of an IIoT deployment [48]. ECSO [24] also describes this framework, and concentrates on outlining the focus of the framework, pointing the existence of the IIC's testbeds for its improvement, and on the relationship of this framework with other best practices;
- **OTA's IoT Security and Privacy Trust Framework v2.5:** The framework [54] is intended to serve as a risk assessment guide for developers, purchasers, and retailers [18]. It provides 44 strategic principles which are grouped into four key areas (i.e., security principles, user access and credentials, privacy, disclosures and transparency, notifications and related best practices), and where each principle is flagged as either "as required" or "recommended" [54]. ECSO [24] also provides a concise description around the focus of this framework.

2.1.3. Manufacturer Specific IoT Security Best Practices

This subsubsection provides an overview of the selected manufacturer specific IoT security best practices. Each of these best practices is outlined below under its corresponding type-based category (i.e., standards, guidelines).

Manufacturer Specific IoT Security Standards

The selected manufacturer specific IoT security standards are outlined below:

- **ETSI European Standard (EN) 303.645 V2.1.1 Cyber Security for Consumer Internet of Things: Baseline Requirements:** This standard [30] consists of outcome-focused provisions (i.e., security and data protection) for developers and manufacturers to secure consumer IoT devices [68]. In addition, these provisions address constrained IoT devices. In addition, this standard provides a list of informative references [30];
- **NEMA's Cyber Hygiene Best Practices:** This standard provides cybersecurity principles for electrical equipment and medical imaging manufacturers that may be implemented in the manufacturing facilities and engineering processes of most manufacturing environments. In addition, for each recommended cybersecurity principle, it provides identification of threats and an analysis of their implications along with reference documents [52].

Manufacturer Specific IoT Security Guidelines

All selected manufacturer specific IoT security guidelines provide manufacturers with security recommendations [43,53], baseline capabilities [26], and principles for IoT devices [49]. The selected guidelines are outlined below:

- **BITAG's Internet of Things (IoT) Security and Privacy Recommendations:** This report [43] addresses security and privacy issues of IoT devices [18], and it provides manufacturers with ten actionable security and privacy recommendations focused on consumer IoT devices [49]. ECSO [24] also provides a brief description around the focus of this guideline;
- **CSDE's The C2 Consensus on IoT Device Security Baseline Capabilities:** Provides manufacturers with thirteen industry consensus security baseline capabilities for IoT devices. Besides these security baseline capabilities, this guideline provides as part of annexes some security capabilities envisaged to become baseline, along with other IoT device security capabilities and practices that are not universally applicable across the IoT ecosystem. Moreover, it enumerates informative references and provides several annexes that map each of the recommended IoT security capabilities against the security requirements of several IoT security best practices (e.g., [28,30,61]) [26];

- **IEEE's Internet of Things (IoT) Security Best Practices:** This report provides IoT manufacturers with eleven prioritized IoT security recommendations for the manufacturing design phase of IoT products. These recommendations are grouped into three categories: securing devices, securing networks, and securing the overall system [49];
- **NIST's Foundational Cybersecurity Activities for IoT Device Manufacturers**: Covers six cybersecurity activities for IoT device manufacturers which are split into two categories: activities related to the premarket phase of IoT devices and activities related to the postmarket phase of IoT devices. For each recommended cybersecurity activity, it provides a list with examples of questions to assist IoT manufacturers as a starting point in achieving the corresponding activity [53].

2.1.4. Supplier Specific IoT Security Best Practices

This subsubsection provides an overview of the selected supplier specific IoT security best practices. Each of these best practices is outlined below under its corresponding type-based category (i.e., codes of practice, guidelines, frameworks).

Supplier Specific IoT Security Codes of Practice

The selected supplier specific IoT security codes of practice provide a set of IoT security measures recommended by the UK Government [61] and Australian Government [42]. These codes of practice are outlined below:

- **UK DCMS's Code of Practice for Consumer IoT Security:** This code of practice [61] provides 13 prioritized guidelines for improving the security of consumer IoT products and associated services, and applies to device manufacturers, IoT service providers, and mobile application developers and retailers [18]. In addition, for each IoT security guideline, the document lists the target stakeholders. In addition, this document (i.e., [61]) is supplemented by a comprehensive mapping document (i.e., [27]) which maps each recommended guideline against related IoT security recommendations, guidance, and standards [68];
- **Australian Government's Code of Practice Securing the Internet of Things for Consumers:** This document aligns with and builds upon the UK DCMS's Code of Practice [61]. It provides a voluntary set of 13 principles as the minimum standard for improving the security of IoT devices and services in Australia and highlights the top three IoT security principles (i.e., no duplicated default or weak passwords, implement a vulnerability disclosure policy, keep software securely updated). In addition, for each recommended IoT security principle, the document lists the target stakeholders which range from device manufacturers to retailers [42].

Supplier Specific IoT Security Guidelines

The selected supplier specific IoT security guidelines are outlined below:

- **AIOTI's Report on Workshop on Security and Privacy in the Hyper-Connected World:** This report provides basic security and privacy requirements on four key areas, including practical privacy in IoT device, IoT hardware and components, interfaces, communication, cloud, and applications [41];
- **U.S. NHTSA's Cybersecurity Best Practices for Modern Vehicles:** This document [60] provides cybersecurity guidance for automotive industry and applies to motor vehicle and motor vehicle equipment designers, suppliers, manufacturers, alterers, and modifiers [18].

Supplier Specific IoT Security Frameworks

The selected supplier specific IoT security frameworks are outlined below:

- **GSMA's IoT Security Assessment Checklist Version 3.0:** This self-assessment checklist document [47] provides a set of general and specific security recommendations for IoT service and endpoint ecosystems, and it applies to IoT service providers, IoT service platform vendors, and IoT device vendors [18]. The general recommendations include IoT security and privacy recommendations at the organizational level (i.e., risks assessments, privacy considerations, secure development), and IoT security recommendations for service platforms and endpoint devices. The specific IoT security recommendations target service platforms and endpoint devices, and are categorized into critical, high, medium, and low priority recommendations. In addition, this self-assessment document allows organizations willing to assess their compliance against its recommendations to rate each of the controls associated with each of the questions of each recommendation [47]. ECSO [24] also mentions the self-assessment checklist and outlines the process for assessing IoT products, services, or components against this checklist;

- **IoTSF's IoT Security Compliance Framework Release 2.1:** It provides a checklist of IoT security requirements which are categorized into 13 groups (e.g., business security processes, policies and responsibilities, device hardware and physical security, device software) [24], and each IoT security requirement is categorized based on its applicability to the system (i.e., software, hardware, and physical) or business components (i.e., process, policy, and responsibility) [50]. In addition, for each IoT security requirement, the framework provides the compliance applicability (i.e., either advisory or mandatory), the required assessment method, and the type of evidence, and expects organizations to fill three fields (i.e., pre-compliance, evidence, responsibility) [50]. This framework is supplemented by a compliance checklist spreadsheet [69] to support the checkbox assessment exercise. A succinct description of this framework is also provided by Garcia-Morchon et al. [18].

2.2. *Methodology for Developing the IoTSRM2*

This subsection describes our methodology used for developing the proposed IoT Security Risk Management Strategy Reference Model (IoTSRM2). Figure 2 shows our proposed three-phased methodology that consists of nine steps and outputs, namely three steps with associated outputs for each of the three phases (i.e., scoping, analysis, and creation).

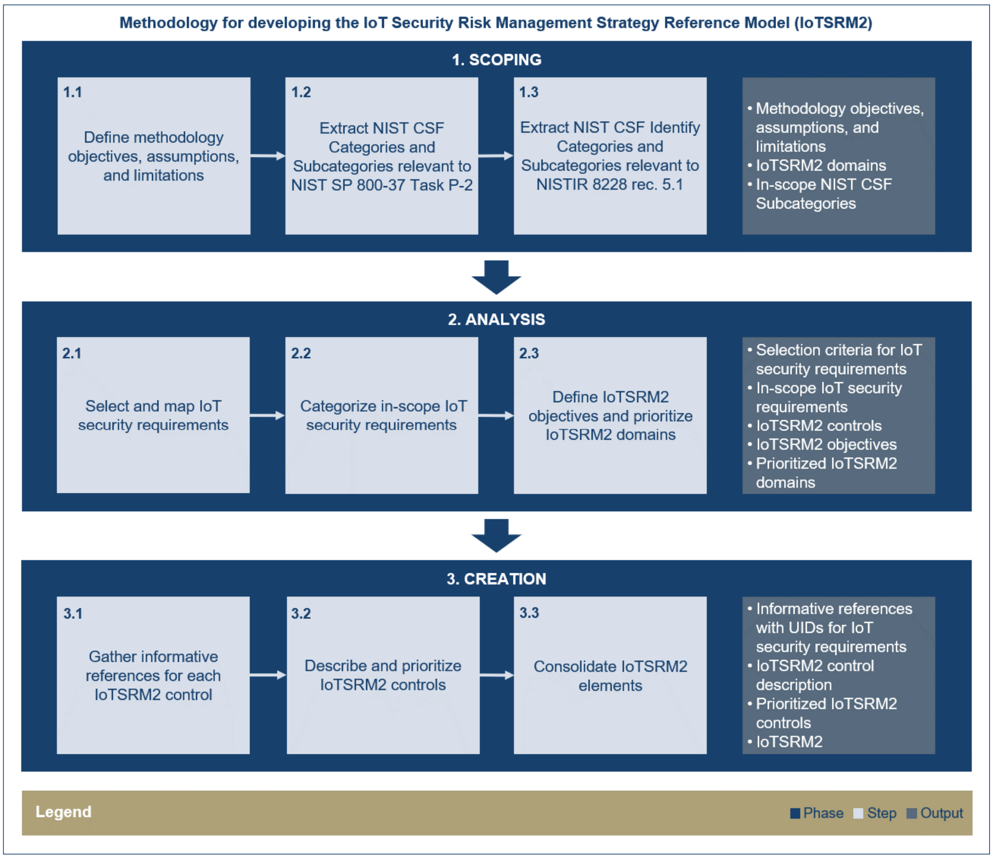
Methodology for developing the IoT Security Risk Management Strategy Reference Model (IoTSRM2)
1. SCOPING
1.1
Define methodology objectives, assumptions, and limitations
1.2
Extract NIST CSF Categories and Subcategories relevant to NIST SP 800-37 Task P-2
1.3
Extract NIST CSF Identify Categories and Subcategories relevant to NISTIR 8228 rec. 5.1
• Methodology objectives, assumptions, and limitations
• IoTSRM2 domains
• In-scope NIST CSF Subcategories
2. ANALYSIS
2.1
Select and map IoT security requirements
2.2
Categorize in-scope IoT security requirements
2.3
Define IoTSRM2 objectives and prioritize IoTSRM2 domains
• Selection criteria for IoT security requirements
• In-scope IoT security requirements
• IoTSRM2 controls
• IoTSRM2 objectives
• Prioritized IoTSRM2 domains
3. CREATION
3.1
Gather informative references for each IoTSRM2 control
3.2
Describe and prioritize IoTSRM2 controls
3.3
Consolidate IoTSRM2 elements
• Informative references with UIDs for IoT security requirements
• IoTSRM2 control description
• Prioritized IoTSRM2 controls
• IoTSRM2
Legend
■ Phase □ Step ■ Output

Figure 2. Our proposed three-phased methodology for developing IoTSRM2.

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

PHASE 1 SCOPING

The scoping phase involves the definition of methodology objectives, assumptions, and limitations (Step 1.1), the establishment of focus domains for IoTSRM2 (Step 1.2), and the determination of the in-scope NIST Cybersecurity Framework (CSF) Subcategories (Step 1.3).

Step 1.1 Define methodology objectives, assumptions, and limitations

First, this step outlines the ten objectives of the proposed methodology. Thus, the main objectives of the proposed methodology are:

- **Objective 1:** Develop a reference model for IoT security risk management strategy applicable to IoT adopters from any sector;
- **Objective 2:** Develop the proposed reference model based on NIST CSF [70] and selected IoT security best practices (see Section 2.1).

Then, to ensure a comprehensive characterization of the granularity of the proposed reference model, the remaining objectives are designed to address both dimensions (i.e., structural granularity and information granularity) of the classification framework for model granularity developed by Maier et al. [71].

In terms of the structural granularity dimension, the objective of the proposed methodology is:

- **Objective 3:** Organize the proposed reference model in hierarchical structures, including domain level, objective level, and control level.

As for the information granularity dimension, the objectives of the proposed methodology are:

- **Objective 4:** Identify IoT security domains to group IoT security objectives for the proposed reference model;
- **Objective 5:** Define high-level IoT security objectives to group IoT security controls for the proposed reference model;
- **Objective 6:** Define the criteria for selecting IoT security requirements from selected IoT security best practices;
- **Objective 7:** Define IoT security controls for the proposed IoT security objectives based on selected IoT security requirements from the in-scope IoT security best practices;
- **Objective 8:** Describe the proposed IoT security controls for IoT adopters using the following levels of detail: expected IoT security related activities/actions from IoT adopters, integration points for expected IoT security related activities/actions with the cybersecurity programs of IoT adopters, and IoT security related activities/actions of IoT suppliers that govern their postmarket activities and that IoT adopters should expect from them;
- **Objective 9:** Provide informative references for each of the proposed IoT security controls, and indicate those informative references that are considered the most relevant to IoT security risk management strategy;
- **Objective 10:** Provide the prioritization rating for each of the proposed IoT security controls.

Furthermore, this step provides the assumptions on which the proposed methodology is based. These assumptions 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 [70];
- IoT adopters are assumed to outsource IoT software development and not engage in in-house IoT software development activities;
- 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.

In addition, Step 1.1 provides the limitations of the proposed methodology. These are enumerated below:

- The proposed methodology is derived, based on, and limited to our professional judgement and selected best practices;
- The proposed methodology is limited to the assumptions on which it is based.

Step 1.2 Extract NIST CSF Categories and Subcategories relevant to NIST SP 800-37 Task P-2

Step 1.2 funnels the NIST CSF Core to focus the proposed reference model on those Categories and Subcategories that are more relevant to Risk Management Strategy. Hence, this step narrows the focus on the NIST CSF Identify Function considering that Task P-2 (Risk Management Strategy) of NIST SP 800-37 aligns with NIST CSF Identify Function [72].

Step 1.3 Extract NIST CSF Identify Categories and Subcategories relevant to NISTIR 8228 rec. 5.1

Step 1.3 further funnels the NIST CSF Identify Function to focus the proposed reference model on those Categories and Subcategories that are more relevant to IoT security. This step further narrows the focus and identifies those Categories and Subcategories of the NIST CSF Identify Function that are more prone to adjustments when it comes to addressing IoT security risk [73]. Hence, it allows the determination of the domains for the IoTSRM2 and the in-scope NIST CSF Subcategories for the IoTSRM2 objectives. Furthermore, the IoTSRM2 domains are represented using Equation (1), where $\mathrm{x_i}$ represents the six domains of IoTSRM2, and C represents the cardinality of $\mathrm{x_i}$:

$$\mathrm{x_i} = \left\{ \begin{array}{c} \text{Asset Management, Business Environment, Governance,} \\ \text{Risk Assessment, Risk Management Strategy,} \\ \text{Supply Chain Risk Management} \end{array} \right\}, \text{ where } \mathrm{C} = |\mathrm{x_i}| = 6,\ \mathrm{i} = [1\ldots\mathrm{C}] \quad (1)$$

PHASE 2 ANALYSIS

Then, the analysis phase involves the selection and mapping of IoT security requirements from the in-scope IoT security best practices (Step 2.1), the categorization of IoT security requirements (Step 2.2), and the definition of IoTSRM2 objectives (Step 2.3).

Step 2.1 Select and map IoT security requirements

This step involves the identification of the in-scope IoT security requirements from 25 selected IoT security best practices (see Section 2.1). First, IoT security requirements are selected by applying on the selected IoT security best practices the selection criteria outlined below:

- **High-level objectives for IoT adopters:** the IoT security requirement is relevant for the development of organizational understanding to manage cybersecurity risks and makes reference to high-level IoT security risk management objectives for IoT adopters;
- **High-level objectives for IoT adopters and high-level postmarket objectives for IoT suppliers:** the IoT security requirement is relevant for the development of organizational understanding to manage cybersecurity risks and makes double reference to both high-level IoT security risk management objectives for IoT adopters and high-level IoT security risk management objectives for IoT suppliers related to the operations/maintenance and/or disposal of IoT devices and/or services for IoT adopters;
- **High-level postmarket objectives for IoT suppliers:** the IoT security requirement is relevant for the development of organizational understanding to manage cybersecurity risks and makes reference to high-level IoT security risk management objectives for IoT suppliers related to the operations/maintenance and/or disposal of IoT devices and/or services for IoT adopters.

Then, the resulting IoT security requirements are analyzed relative to the in-scope NIST CSF Subcategories from Step 1.3 to determine the in-scope IoT security requirements. Hence, the IoT security requirements are mapped against the in-scope NIST CSF Subcategories from Step 1.3.

Step 2.2 Categorize in-scope IoT security requirements

Step 2.2 involves the grouping of related in-scope IoT security requirements from Step 2.1 under the in-scope NIST CSF Subcategories from Step 1.3. This grouping is made so that any in-scope IoT security requirement appears only once as part of the same in-scope NIST CSF Subcategory. Thus, the in-scope IoT security requirements are captured as part of the most appropriate group of the same in-scope NIST CSF Subcategory to ensure the creation of different categories and enable a more unbiassed prioritization of the proposed IoTSRM2 controls. These groups allow the naming of IoTSRM2 controls (see Section 3.1).

Step 2.3 Define IoTSRM2 objectives and prioritize IoTSRM2 domains

This step involves the definition of IoTSRM2 objectives based on in-scope NIST CSF Subcategories from Step 1.3, the mapping of IoTSRM2 objectives to in-scope NIST CSF Subcategories, and the prioritization of IoTSRM2 domains based on the number of IoTSRM2 objectives corresponding to each IoTSRM2 domain. Thus, the name of each in-scope NIST CSF Subcategory from Step 1.3 is refined based on its corresponding IoTSRM2 controls from Step 2.2 to define each IoTSRM2 objective (see Section 3.1). The IoTSRM2 objectives are represented using the equations from (2) to (7):

- x_{1j} represents the two objectives of the "Asset Management" domain of IoTSRM2 (i.e., x_1), C_1 represents the cardinality of x_{1j}, and n_{1j} represents the number of IoTSRM2 controls corresponding to each objective of this IoTSRM2 domain:

$$x_{1j} = \left\{ \begin{array}{c} \text{Hardware inventory,} \\ \text{Software inventory} \end{array} \right\}, \text{ where } C_1 = |x_{1j}| = 2,\ j = [1 \ldots C_1],\ n_{1j} = \{1, 1\} \tag{2}$$

- x_{2j} represents the two objectives of the "Business Environment" domain of IoTSRM2 (i.e., X_2), C_2 represents the cardinality of x_{2j}, and n_{2j} represents the number of IoTSRM2 controls corresponding to each objective of this IoTSRM2 domain:

$$x_{2j} = \left\{ \begin{array}{c} \text{Dependencies and critical functions,} \\ \text{Critical service resilience} \end{array} \right\}, \text{ where } C_2 = |x_{2j}| = 2,\ j = [1 \ldots C_2],\ n_{2j} = \{1, 1\} \tag{3}$$

- x_{3j} represents the four objectives of the "Governance" domain of IoTSRM2 (i.e., x_3), C_3 represents the cardinality of x_{3j}, and n_{3j} represents the number of IoTSRM2 controls corresponding to each objective of this IoTSRM2 domain:

$$x_{3j} = \left\{ \begin{array}{c} \text{Security related policies,} \\ \text{Structures and responsibilities,} \\ \text{Regulatory requirements,} \\ \text{Governance and risk management plans} \end{array} \right\}, \text{where } C_3 = |x_{3j}| = 4,\ j = [1 \ldots C_3],\ n_{3j} = \{4, 2, 1, 7\} \tag{4}$$

- x_{4j} represents the four objectives of the "Risk Assessment" domain of IoTSRM2 (i.e., x_4), C_4 represents the cardinality of x_{4j}, and n_{4j} represents the number of IoTSRM2 controls corresponding to each objective of this IoTSRM2 domain:

$$x_{4j} = \left\{ \begin{array}{c} \text{Vulnerability discovery,} \\ \text{Threat identification,} \\ \text{Risk analysis,} \\ \text{Risk responses} \end{array} \right\}, \text{ where } C_4 = |x_{4j}| = 4,\ j = [1 \ldots C_4],\ n_{4j} = \{2, 2, 1, 1\} \tag{5}$$

- x_{5j} represents the two objectives of the "Risk Management Strategy" domain of IoTSRM2 (i.e., x_5), C_5 represents the cardinality of x_{5j}, and n_{5j} represents the number of IoTSRM2 controls corresponding to each objective of this IoTSRM2 domain:

$$x_{5j} = \left\{ \begin{array}{c} \text{Risk appetite and tolerances,} \\ \text{Context-informed risk tolerances} \end{array} \right\}, \text{ where } C_5 = |x_{5j}| = 2,\ j = [1 \ldots C_5],\ n_{5j} = \{1, 1\} \tag{6}$$

- x_{6j} represents the two objectives of the "Supply Chain Risk Management" domain of IoTSRM2 (i.e., x_6), C_6 represents the cardinality of x_{6j}, and n_{6j} represents the number of IoTSRM2 controls corresponding to each objective of this IoTSRM2 domain:

$$x_{6j} = \left\{ \begin{array}{c} \text{Supplier assessment,} \\ \text{Supplier contract management} \end{array} \right\}, \text{ where } C_6 = |x_{6j}| = 2,\ j = [1 \ldots C_6],\ n_{6j} = \{2, 2\} \tag{7}$$

Each of these IoTSRM2 objectives is considered to have the same weight across IoTSRM2 domains to avoid placing more importance on some objectives than others and to enable any organization to leverage the IoTSRM2 regardless of their risk appetites and IoT security risk tolerances. Thus, Equation (8) provides the weight of each IoTSRM2 objective:

$$\text{Weight } (x_{ij}) = \frac{1}{\sum_1^C C_q}, \text{ where } i = [1 \ldots C],\ j = [1 \ldots C_i],\ \sum_1^{\sum_1^C C_q} \frac{1}{\sum_1^C C_q} = 100\% \tag{8}$$

Then, the IoTSRM2 domains are prioritized using the following formula:

$$\text{Weight } (x_i) = \frac{C_i}{\sum_1^C C_q}, \text{ where } i = [1 \ldots C], \sum_{i=1}^{C} \frac{C_i}{\sum_1^C C_q} = 100\% \tag{9}$$

PHASE 3 CREATION

Then, the creation phase involves the collection of informative references for each IoTSRM2 control (Step 3.1), the description and prioritization of proposed IoTSRM2 controls (Step 3.2), and the consolidation of the IoTSRM2 elements (Step 3.3).

Step 3.1 Gather informative references for each IoTSRM2 control

For each IoTSRM2 control, this step involves the gathering and documentation of applicable informative references with associated unique identifiers (UIDs) of the in-scope IoT security requirements from Step 2.1 (see Section 3.1). These informative references and unique identifiers show that there is a link between the proposed IoTSRM2 and the selected IoT security best practices, provide further context on secure IoT adoption, and are intended to help IoT adopters to formulate or rethink their IoT security risk management strategies. Notwithstanding, the sole implementation of the IoT security requirements from the informative references does not necessarily lead to IoTSRM2 compliance.

Step 3.2 Describe and prioritize IoTSRM2 controls

First, this step involves the description of IoTSRM2 controls from Step 2.2 to achieve the methodology objectives and to reflect cybersecurity and IoT security risk management best practices (see Section 3.1). Then, the IoTSRM2 controls are prioritized for each IoTSRM2 objective based on their corresponding adjusted weights which are determined using Equations (10) and (11).

Equation (10) allows the determination of the IoTSRM2 control weights. This equation takes into account the average in-scope IoT security requirements per an applicable informative reference to address some of the duplicates, and the number of in-scope IoT security requirements relative to the number of selected IoT security best practices to lift the weight of those IoTSRM2 controls that capture more in-scope IoT security requirements than others. In this equation, x_{ijk} represents the controls of the x_{ij} objectives of the x_i domains of IoTSRM2, $R\left(x_{ijk}\right)$ represents the number of in-scope IoT security requirements applicable for each of the x_{ijk} controls of each of the x_{ij} objectives of each of the x_i domains of IoTSRM2, $I\left(x_{ijk}\right)$ represents the number of informative references applicable for each of the x_{ijk} controls of each of the x_{ij} objectives of each of the x_i domains of IoTSRM2, and p represents the number of selected IoT security best practices (see Section 2.1).

$$\text{Weight } \left(x_{ijk}\right) = \frac{R\left(x_{ijk}\right)}{I\left(x_{ijk}\right)} + \frac{R\left(x_{ijk}\right)}{p}, \text{ where } i = [1 \ldots C],\ j = [1 \ldots C_i],\ k = \left[1 \ldots n_{ij}\right] \tag{10}$$

Then, the resulting control weights are adjusted using Equation (11) to ensure normalization of values so that the weights of the IoTSRM2 controls of any IoTSRM2 objective add up to 100%:

$$\text{Adjusted weight}\left(\mathrm{x_{ijk}}\right) = \frac{1}{\sum_1^{\mathrm{C}} \mathrm{C_q}} * \frac{\text{Weight}\left(\mathrm{x_{ijk}}\right)}{\sum_{\mathrm{s}=1}^{\mathrm{n_{ij}}} \text{Weight}\left(\mathrm{x_{ijs}}\right)} * 100\%,$$
$$\text{where } \mathrm{i} = [1 \ldots \mathrm{C}],\ \mathrm{j} = [1 \ldots \mathrm{C_i}],\ \mathrm{k} = [1 \ldots \mathrm{n_{ij}}],\ \sum_{\mathrm{i}=1}^{\mathrm{C}} \sum_{\mathrm{j}=1}^{\mathrm{C_i}} \sum_{\mathrm{k}=1}^{\mathrm{n_{ij}}} \text{Adjusted weight}\left(\mathrm{x_{ijk}}\right) = 100\% \tag{11}$$

Step 3.3 Consolidate IoTSRM2 elements

To showcase the proposed IoTSRM2 (see Section 3.1), Step 3.3 brings together the following IoTSRM2 elements, not necessarily in that order:

- IoTSRM2 domains, objectives, and controls;
- for each IoTSRM2 control, applicable informative references with associated unique identifiers of the in-scope IoT security requirements;
- for each IoTSRM2 objective, the prioritization of IoTSRM2 controls based on their corresponding adjusted weights;
- for each informative reference of IoTSRM2, the total number of in-scope IoT security requirements mapped, and the indication as to whether it classifies among the informative references that are considered the most relevant to IoT security risk management strategy.

Note that, to classify among the informative references of IoTSRM2 that are considered the most relevant to IoT security risk management strategy, the informative references are selected to meet the following two inclusion criteria and two conditions:

- **Inclusion criterion 1:** the informative references (i.e., type 1) that are the most focused on IoT security risk management strategy based on the percentage of unique IoT security requirements applicable to IoTSRM2 of each informative reference of the total number of IoT security requirements of the informative reference in question;
- **Inclusion criterion 2**: the informative references (i.e., type 2) that are the most applicable to the proposed IoTSRM2 based on the percentage of all IoT security requirements applicable to IoTSRM2 of each informative reference of the total number of IoT security requirements applicable to IoTSRM2 of all 25 informative references;
- **Condition 1:** for each informative reference of type 1, to include an informative reference of type 2 irrespective of whether the resulting informative references are the same;
- **Condition 2**: to include as many pairs of type 1 and type 2 informative references as needed, so that the total number of all IoT security requirements applicable to IoTSRM2 of the selected unique informative references to amount to at least 50% of the total number of IoT security requirements applicable to IoTSRM2 of all 25 informative references.

3. Results

This section is structured in two subsections. Section 3.1 presents our proposed IoTSRM2. First, it provides an illustrative overview of the proposed IoTSRM2. Second, it enumerates the seven selected informative references together with their corresponding total number of unique in-scope IoT security requirements mapped to IoTSRM2. Third, for each IoTSRM2 domain, it provides the IoTSRM2 objectives and, for each IoTSRM2 objective, it provides the description of and the informative references for each IoTSRM2 control, followed by the prioritization of the IoTSRM2 controls for each IoTSRM2 objective. Subsequently, Section 3.2 provides the critical evaluation of the selected informative references of IoTSRM2 based on their percentage-wise linkage to IoTSRM2.

3.1. Our Proposed IoTSRM2

Based on the 25 selected IoT security best practices outlined in Section 2.1 and on our methodology introduced in Section 2.2, this subsection provides our proposed IoT security risk management strategy reference model (IoTSRM2) which is the main contribution of this research article as it bridges one major research gap in IoT security risk management strategy, namely the absence of a reference model for IoT security risk management strategy. First, Figure 3 illustrates the IoTSRM2 domains, objectives, and controls for IoT adopters, which should be addressed by both IoT adopters and IoT suppliers, and it indicates two IoTSRM2 controls that IoT adopters should review to establish whether these two are adequately implemented by IoT suppliers. As depicted in Figure 3, our proposed IoTSRM2 consists of six domains, sixteen objectives, and thirty controls. This depiction provides a consolidated view of the key elements of IoTSRM2 that allows IoT adopters to achieve a high-level understanding of the IoTSRM2 domains, objectives, and controls which should be considered by them while framing or reframing their IoT security risk management strategies. This illustrative overview can be availed by IoT security practitioners and researchers before diving deeper into the IoTSRM2 domains, objectives and controls when crafting robust IoT security risk management strategies and engaging in IoT security risk management strategy-related research undertakings, respectively.

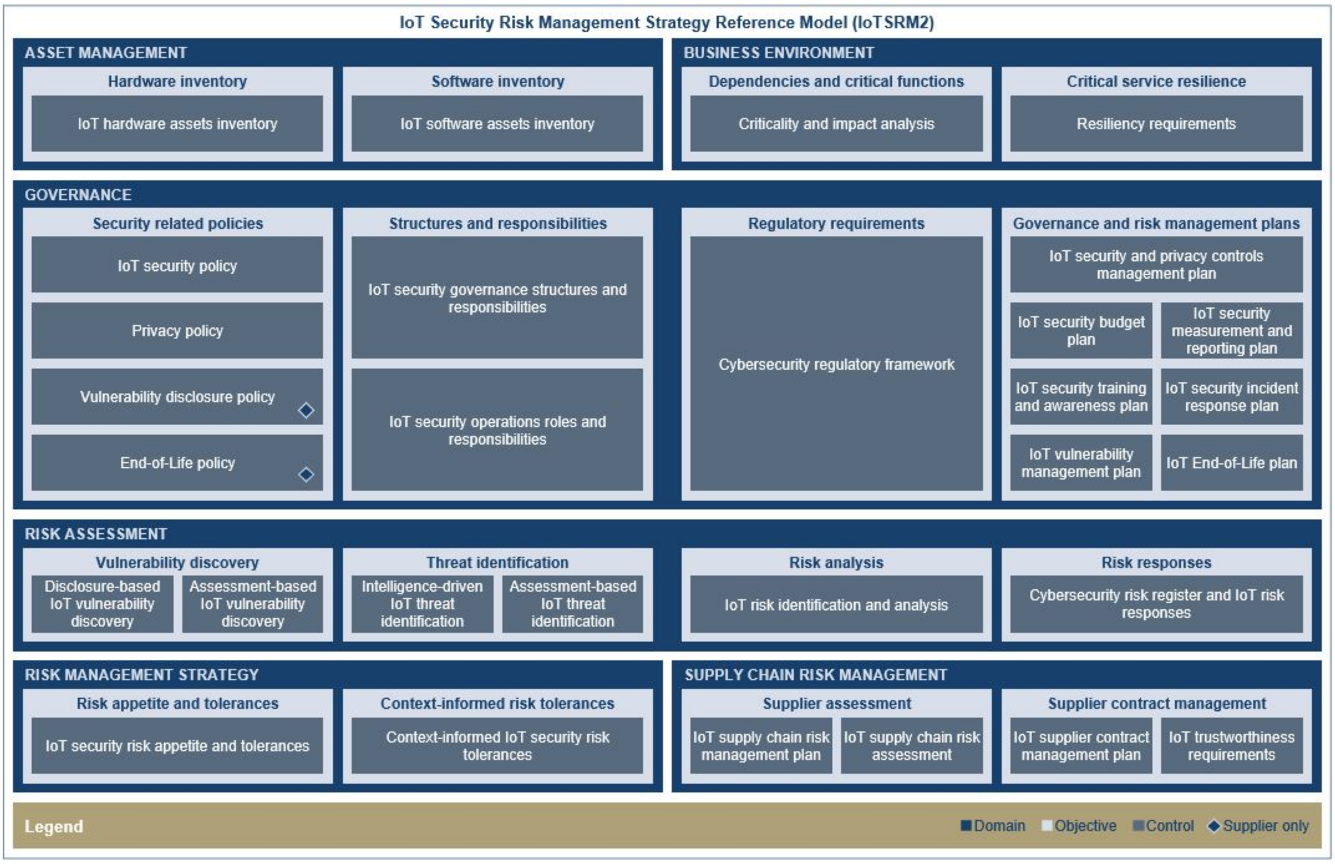
IoT Security Risk Management Strategy Reference Model (IoTSRM2)
ASSET MANAGEMENT
Hardware inventory
IoT hardware assets inventory
Software inventory
IoT software assets inventory
BUSINESS ENVIRONMENT
Dependencies and critical functions
Criticality and impact analysis
Critical service resilience
Resiliency requirements
GOVERNANCE
Security related policies
IoT security policy
Privacy policy
Vulnerability disclosure policy ◆
End-of-Life policy ◆
Structures and responsibilities
IoT security governance structures and responsibilities
IoT security operations roles and responsibilities
Regulatory requirements
Cybersecurity regulatory framework
Governance and risk management plans
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
IoT vulnerability management plan
IoT End-of-Life plan
RISK ASSESSMENT
Vulnerability discovery
Disclosure-based IoT vulnerability discovery
Assessment-based IoT vulnerability discovery
Threat identification
Intelligence-driven IoT threat identification
Assessment-based IoT threat identification
Risk analysis
IoT risk identification and analysis
Risk responses
Cybersecurity risk register and IoT risk responses
RISK MANAGEMENT STRATEGY
Risk appetite and tolerances
IoT security risk appetite and tolerances
Context-informed risk tolerances
Context-informed IoT security risk tolerances
SUPPLY CHAIN RISK MANAGEMENT
Supplier assessment
IoT supply chain risk management plan
IoT supply chain risk assessment
Supplier contract management
IoT supplier contract management plan
IoT trustworthiness requirements
Legend
■Domain
□Objective
■Control
◆Supplier only

Figure 3. Our proposed IoTSRM2.

Then, Table 3 lists the informative references of IoTSRM2 that are considered the most relevant to IoT security risk management strategy from the 25 informative references of IoTSRM2, and it shows the total number of unique in-scope IoT security requirements mapped against the IoTSRM2, of each selected informative reference. These seven informative references resulted in being the most relevant to IoT security risk management strategy as they meet the two inclusion criteria and two conditions from Step 3.3 of our proposed methodology outlined in Section 2.2.

Furthermore, for each IoTSRM2 domain, this subsection provides the associated IoTSRM2 objectives. Additionally, for each IoTSRM2 objective, it describes the IoTSRM2 controls consistent with the intended information granularity from our methodology for developing the IoTSRM2 (see Section 2.2). Moreover, for each IoTSRM2 control, it provides the corresponding informative references and the unique identifiers of the in-scope IoT security requirements that are applicable, of each selected informative reference. In addition, for each objective of each IoTSRM2 domain, this subsection provides the unique identifier of the corresponding in-scope NIST CSF Subcategory, and the prioritization of IoTSRM2 controls based on their adjusted weights. The adjusted weights of the IoTSRM2 controls are provided in Tables 4–9. It is worth noting that the adjusted weight for each IoTSRM2 control is calculated using Equations (10) and (11) (see Section 2.2).

Table 3. Selected informative references.

Informative Reference	Name of Informative Reference	Total # of Unique in-Scope IoT Security Requirements Mapped
[55]	ENISA’s Good Practices for Security of Internet of Things in the context of Smart Manufacturing	54
[46]	CSA IoT Security Controls Framework Version 1	41
[50]	IoTSF’s IoT Security Compliance Framework Release 2.1	34
[40]	AgeLight’s IoT Safety Architecture & Risk Toolkit v4.0	31
[57]	ENISA’s Procurement Guidelines for Cybersecurity in Hospitals Good practices for the security of Healthcare services	23
[51]	Japan’s IoTAC IoT Security Guidelines Ver. 1.0	12
[53]	NIST’s Foundational Cybersecurity Activities for IoT Device Manufacturers	9

Table 4. Prioritized IoTSRM2 controls for each objective of the “Asset Management” domain.

IoTSRM2 Objective	NIST CSF Subcateg. ID	IoTSRM2 Control	Adjusted Control Weight
Hardware inventory (AM.A)	ID.AM-1	IoT hardware assets inventory (AM.A.1)	6.25%
Software inventory (AM.B)	ID.AM-2	IoT software assets inventory (AM.B.1)	6.25%

Table 5. Prioritized IoTSRM2 controls for each objective of the “Business Environment” domain.

IoTSRM2 Objective	NIST CSF Subcateg. ID	IoTSRM2 Control	Adjusted Control Weight
Dependencies and critical functions (BE.A)	ID.BE-4	Criticality and impact analysis (BE.A.1)	6.25%
Critical service resilience (BE.B)	ID.BE-5	Resiliency requirements (BE.B.1)	6.25%

Table 6. Prioritized IoTSRM2 controls for each objective of the "Governance" domain.

IoTSRM2 Objective	NIST CSF Subcateg. ID	IoTSRM2 Control	Adjusted Control Weight
Security related policies (GV.A)	ID.GV-1	IoT security policy (GV.A.1)	2.20%
		Privacy policy (GV.A.2)	1.67%
		Vulnerability disclosure policy (GV.A.3)	1.23%
		End-of-Life policy (GV.A.4)	1.15%
Structures and responsibilities (GV.B)	ID.GV-2	IoT security governance structures and responsibilities (GV.B.1)	3.29%
		IoT security operations roles and responsibilities (GV.B.2)	2.96%
Regulatory requirements (GV.C)	ID.GV-3	Cybersecurity regulatory framework (GV.C.1)	6.25%
Governance and risk management plans (GV.D)	ID.GV-4	IoT security and privacy controls management plan (GV.D.1)	2.14%
		IoT security training and awareness plan (GV.D.4)	0.96%
		IoT vulnerability management plan (GV.D.6)	0.89%
		IoT security budget plan (GV.D.2)	0.67%
		IoT End-of-Life plan (GV.D.7)	0.63%
		IoT security incident response plan (GV.D.5)	0.62%
		IoT security measurement and reporting plan (GV.D.3)	0.35%

Table 7. Prioritized IoTSRM2 controls for each objective of the "Risk Assessment" domain.

IoTSRM2 Objective	NIST CSF Subcateg. ID	IoTSRM2 Control	Adjusted Control Weight
Vulnerability discovery (RA.A)	ID.RA-1	Assessment-based IoT vulnerability discovery (RA.A.2)	4.56%
		Disclosure-based IoT vulnerability discovery (RA.A.1)	1.69%
Threat identification (RA.B)	ID.RA-3	Assessment-based IoT threat identification (RA.B.2)	4.62%
		Intelligence-driven IoT threat identification (RA.B.1)	1.63%
Risk analysis (RA.C)	ID.RA-4	IoT risk identification and analysis (RA.C.1)	6.25%
Risk responses (RA.D)	ID.RA-6	Cybersecurity risk register and IoT risk responses (RA.D.1)	6.25%

Table 8. Prioritized IoTSRM2 controls for each objective of the "Risk Management Strategy" domain.

IoTSRM2 Objective	NIST CSF Subcateg. ID	IoTSRM2 Control	Adjusted Control Weight
Risk appetite and tolerances (RM.A)	ID.RM-2	IoT security risk appetite and tolerances (RM.A.1)	6.25%
Context-informed risk tolerances (RM.B)	ID.RM-3	Context-informed IoT security risk tolerances (RM.B.1)	6.25%

Table 9. Prioritized IoTSRM2 controls for each objective of the "Supply Chain Risk Management" domain.

IoTSRM2 Objective	NIST CSF Subcateg. ID	IoTSRM2 Control	Adjusted Control Weight
Supplier assessment (SC.A)	ID.SC-2	IoT supply chain risk management plan (SC.A.1)	3.90%
		IoT supply chain risk assessment (SC.A.2)	2.35%
Supplier contract management (SC.B)	ID.SC-3	IoT trustworthiness requirements (SC.B.2)	4.20%
		IoT supplier contract management plan (SC.B.1)	2.05%

A consolidated view of IoTSRM2 controls with informative references is provided in Appendix A as part of Table A1.

Asset Management (AM)

The "Asset Management" domain of IoTSRM2 comprises the following two objectives:

- Hardware inventory (AM.A): Determine whether IoT hardware assets are inventoried;
- Software inventory (AM.B): Determine whether IoT software assets are inventoried.

Hardware Inventory (AM.A)

The "Hardware inventory" objective has one IoTSRM2 control, namely "IoT hardware assets inventory" control.

IoT hardware assets inventory (AM.A.1): IoT devices and their hardware components are discovered, inventoried, assigned owners, classified, and tracked throughout their lifecycles using a centralized, formally approved, periodically reviewed, and up-to-date IT inventory which is synchronized with the configuration management database (CMDB) that feeds the organization's data warehouse. The activities of discovering, inventorying, and tracking IoT hardware assets are aligned with and part of wider IoT hardware asset management and IT asset management processes. The organization's IoT suppliers manage their hardware assets across their lifecycles and provide cybersecurity bills of materials (CBOMs) to IoT adopters for the IoT products they acquire.

The informative references for this IoTSRM2 control are [30]; [40]: 12; [44,45]; [46]: ACT-01, ACT-03, ACT-04, ACT-05, GVN-01, OPA-01, TSP-02; [53]: 4.2.3, 4.2.6; [54]; [55]: PS-11, PS-12, PS-14; [57]: GP 28; [58,59].

Software inventory (AM.B)

The "Software inventory" objective has one IoTSRM2 control, namely "IoT software assets inventory" control.

IoT software assets inventory (AM.B.1): All software assets relevant to IoT devices and/or services are discovered, inventoried, assigned owners, classified, and tracked throughout their lifecycles using a centralized, formally approved, periodically reviewed, and up-to-date IT inventory which is synchronized with the configuration management database (CMDB) that feeds the organization's data warehouse. The activities of discovering, inventorying, and tracking IoT software assets are aligned with and part of wider IoT software asset management and IT asset management processes. The organization's IoT suppliers manage their software assets across their lifecycles and provide cybersecurity bills of materials (CBOMs) to IoT adopters for acquired IoT products.

The informative references for this IoTSRM2 control are [40]: 12; [44]; [46]: ACT-01, ACT-03, ACT-05, GVN-01, TSP-02; [51]: Principle 2: Key concept 3; [53]: 4.2.3, 4.2.6; [54]; [55]: PS-11, PS-12, PS-14; [57]: GP 28; [58,59].

Then, for each IoTSRM2 objective of the "Asset Management" domain, Table 4 provides the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 control with its adjusted weight. These IoTSRM2 controls are already prioritized within each IoTSRM2 objective given that there is only one control for each objective, and in effect the adjusted weight of each IoTSRM2 control is the same as the weight of the associated IoTSRM2 objective.

Business Environment (BE)

The "Business Environment" domain of IoTSRM2 consists of the following two objectives:

- Dependencies and critical functions (BE.A): Determine whether dependencies and critical functions for delivery of critical IoT enabled services are established;
- Critical service resilience (BE.B): Determine whether resilience requirements to support delivery of critical IoT enabled services are established.

Dependencies and critical functions (BE.A)

The "Dependencies and critical functions" objective has one IoTSRM2 control, namely "Criticality and impact analysis" control.

Criticality and impact analysis (BE.A.1): All IoT enabled services (e.g., internal services, customer services) along with the enablers of the organization's IoT infrastructure (e.g., components and subcomponents, business services, IT and OT infrastructure, IoT supply chain) are identified, analyzed, and prioritized based on their relative importance to organizational resilience and stakeholders. These activities of assessing IoT enabled services and enablers are aligned with and part of overarching cybersecurity risk management program. The organization's IoT suppliers undertake regular dependency and criticality analysis that inform their system development lifecycles, and they provide cybersecurity bills of materials (CBOMs) to IoT adopters for the IoT products they acquire.

The informative references for this IoTSRM2 control are [28]; [40]: 12, 23, 44; [41]; [46]: GVN-02, SOP-01, SOP-02, TMM-04; [48]; [51]: Principle 2: Key concept 3, Principle 2: Key concept 5, Principle 5: Key concept 19; [53]: 4.2.1, 4.2.3, 4.2.6; [54]; [55]: PS-07, PS-08, PS-19, TM-10, TM-13; [56]; [57]: GP 7, GP 12; [58–60].

Critical service resilience (BE.B)

The "Critical service resilience" objective has one IoTSRM2 control, namely "Resiliency requirements" control.

Resiliency requirements (BE.B.1): Cybersecurity, reliability, continuity, and recovery requirements for critical IoT enabled services across the entire disruption lifecycle, are established, documented, formally approved, periodically reviewed, and up-to-date. These resiliency requirements for all mission critical IoT enabled services derived from criticality and impact analysis are in line with the risk tolerances and established based on applicable regulatory obligations and operational resilience best practices as part of the organization's cybersecurity controls management, cybersecurity incident response, and business continuity and disaster recovery plans. The organization's IoT suppliers have robust system development lifecycles that incorporate resiliency requirements, communicate their cybersecurity incident response, service continuity, and disaster recovery plans to IoT adopters, and provide cybersecurity bills of materials (CBOMs) to IoT adopters for the IoT products they acquire.

The informative references for this IoTSRM2 control are [28]; [40]: 12, 23, 44; [44,45]; [46]: BCN-01; [48]; [50]: 2.4.3.18, 2.4.3.23; [52,54]; [55]: OP-01, TM-09, TM-12, TM-15, TM-16, TM-17; [56]; [57]: GP 6, GP 17, GP 22, GP 23; [58–60].

Then, for each IoTSRM2 objective of the "Business Environment" domain, Table 5 provides the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 control with its adjusted weight. These IoTSRM2 controls are already prioritized within each IoTSRM2 objective given that there is only one control for each objective, and in effect the adjusted weight of each IoTSRM2 control is the same as the weight of the associated IoTSRM2 objective.

Governance (GV)

The "Governance" domain of IoTSRM2 consists of the following four objectives:

- Security related policies (GV.A): Determine whether the IoT security related policies are established and communicated;
- Structures and responsibilities (GV.B): Determine whether the IoT security risk management structures, responsibilities, and shared responsibilities are established;
- Regulatory requirements (GV.C): Determine whether cybersecurity-related regulatory requirements are understood and managed;

- Governance and risk management plans (GV.D): Determine whether governance and risk management plans address IoT security risks.

Security related policies (GV.A)

The "Security related policies" objective has four IoTSRM2 controls.

IoT security policy (GV.A.1): An organization-wide IoT security policy, which is aligned with and part of wider overarching cybersecurity policy, is clearly defined, documented, approved by board committees and/or C-suite executives, periodically reviewed, up-to-date, and well communicated. This policy incorporates IoT security requirements relevant for the protection of confidentiality, integrity, availability, and safety of organizational assets (i.e., staff and third parties, processes, technology, data, and facilities). The organization's IoT suppliers have and maintain cybersecurity policies incorporating IoT security considerations, and they communicate these policies to IoT adopters.

The informative references for this IoTSRM2 control are [28,30]; [40]: 4, 5, 7; [41–44]; [46]: TSP-04; [47,48]; [50]: 2.4.3.4, 2.4.3.5, 2.4.3.6, 2.4.8.10; [51]: Principle 1: Key concept 1, Principle 1: Key concept 2; [55]: PS-18; [56]; [57]: GP 3, GP 5; [61].

Privacy policy (GV.A.2): An organization-wide privacy policy, which is aligned with and part of wider overarching data protection policy, is documented, formally approved, published, periodically reviewed, up-to-date, and well communicated. This policy is revised to incorporate IoT privacy requirements for personal data at rest, in transit, and in use. The organization's IoT suppliers have and maintain general privacy policies along with relevant privacy supplements for each IoT product and/or service they provide, and they communicate these policies to IoT adopters.

The informative references for this IoTSRM2 control are [28,30]; [40]: 20, 22, 24, 25, 32, 35, 36; [42–44,47]; [50]: 2.4.12.5; [53]: 4.2.3; [54]; [55]: PS-06; [57]: GP 10; [61].

Vulnerability disclosure policy (GV.A.3): The organization's IoT suppliers have vulnerability disclosure policies that are clearly documented, publicly available, periodically reviewed, up-to-date, and well communicated. These policies are aligned with and part of the vulnerability disclosure program.

The informative references for this IoTSRM2 control are [28,30,42]; [46]: SDV-05; [49]; [50]: 2.4.3.11, 2.4.3.12, 2.4.3.13, 2.4.3.14, 2.4.3.16, 2.4.3.17; [53]: 4.2.6; [59–61].

End-of-Life policy (GV.A.4): The organization's IoT suppliers have End-of-Life policies that are published, easily accessible, periodically reviewed, up-to-date, and well communicated to IoT adopters. These policies are aligned with and part of wider product and/or service lifecycle management strategies.

The informative references for this IoTSRM2 control are [26,28,30]; [40]: 1, 21; [42]; [46]: EOL-01; [49]; [50]: 2.4.5.22, 2.4.5.35; [53]: 4.2.2, 4.2.5; [54,61].

Structures and responsibilities (GV.B)

The "Structures and responsibilities" objective has two IoTSRM2 controls.

IoT security governance structures and responsibilities (GV.B.1): IoT security governance structures and responsibilities across and within the three lines of defense (3LoD) are clearly articulated, documented, board-approved, periodically reviewed, and up-to-date as part of the IoT security risk management program and wider cybersecurity risk management program. The organization's IoT suppliers have established their cybersecurity governance structures and responsibilities, and they work with IoT adopters to define shared governance structures and responsibilities for cybersecurity risk management.

The informative references for this IoTSRM2 control are [46]: GVN-01, UPD-01; [47]; [50]: 2.4.3.1, 2.4.3.2.

IoT security operations roles and responsibilities (GV.B.2): IoT security operations roles, responsibilities, and levels of authority within the first line of defense are clearly articulated, documented, formally approved, periodically reviewed, and up-to-date as part of IoT security risk management program and wider cybersecurity risk management program. The organization's IoT suppliers have established cybersecurity operations' roles and responsibilities, dialogue on shared responsibility for IoT security with IoT adopters, and provide points of contact for IoT security incident response and vulnerability disclosure.

The informative references for this IoTSRM2 control are [28,42,44]; [46]: BCN-01, IMT-02; [47]; [50]: 2.4.3.19, 2.4.3.20, 2.4.3.21, 2.4.12.12; [51]: Principle 5: Key concept 20; [53]: 4.2.1, 4.2.4; [55]: OP-08, OP-11; [56]; [57]: GP 1; [60,61].

Regulatory requirements (GV.C)

The "Regulatory requirements" objective has one IoTSRM2 control, namely "Cybersecurity regulatory framework" control.

Cybersecurity regulatory framework (GV.C.1): A cybersecurity regulatory framework, which captures relevant cybersecurity, data privacy, and IoT security regulatory requirements, is documented, formally approved, periodically reviewed, and up-to-date. This is aligned with and part of wider organization's legal and regulatory framework. The organization's IoT suppliers have and maintain cybersecurity regulatory frameworks which incorporate relevant cybersecurity, data privacy, and IoT security regulatory requirements, and they communicate to IoT adopters about their compliance with applicable legal and regulatory obligations.

The informative references for this IoTSRM2 control are [28]; [40]: 31; [44]; [46]: CLS-04, GVN-02, RSM-01; [47,48,54]; [55]: PS-06, TM-07.

Governance and risk management plans (GV.D)

The "Governance and risk management plans" objective has seven IoTSRM2 controls.

IoT security and privacy controls management plan (GV.D.1): An organization-wide IoT security and privacy controls management plan, which is aligned with and part of the organization's cybersecurity risk management program, is documented, approved by board committees and/or C-suite executives, periodically reviewed, and up-to-date. The organization's IoT suppliers have and maintain controls management plans for improving their cybersecurity postures, and cybersecurity and privacy controls frameworks that enable secure IoT system development lifecycle.

The informative references for this IoTSRM2 control are [28,30]; [40]: 5, 25, 30; [42,44,45]; [46]: BCN-01, RSM-01, SDV-15, UPD-03; [47,48]; [50]: 2.4.3.4, 2.4.12.6, 2.4.12.7, 2.4.16.1, 2.4.12.9, 2.4.12.10, 2.4.16.2; [55]: PS-01, PS-06, PS-16, PS-18, PS-20, PS-22, PS-24, OP-03, OP-06, OP-07, OP-09, OP-24, OP-25, TM-12, TM-14, TM-15, TM-16, TM-40, TM-57; [56]; [57]: GP 6; [58,61].

IoT security budget plan (GV.D.2): A budget plan for the IoT security risk management program is documented, approved by board committees and/or C-suite executives, periodically reviewed, and up-to-date. This plan is part of the cybersecurity budget plan and in line with the overall capital planning and investment control process for IT investments. The organization's IoT suppliers have and maintain cybersecurity budget plans for secure IoT system development lifecycle.

The informative references for this IoTSRM2 control are [28,56,60].

IoT security measurement and reporting plan (GV.D.3): IoT security measurement and reporting plan, which is aligned with and part of wider cybersecurity program measurement and reporting, is defined, documented, formally approved, periodically reviewed, and up-to-date. The organization's IoT suppliers have and maintain plans that cover the definition of security metrics for measuring the performance of IoT services against Service Level Objectives (SLOs), and the means for metrics reporting including dashboards and communication plans.

The informative references for this IoTSRM2 control are [48]; [53]: 4.1; [56,58].

IoT security training and awareness plan (GV.D.4): An organization-wide IoT security training and awareness plan, which is aligned with and part of the organization's cybersecurity training and awareness program, is documented, formally approved, periodically reviewed, and up-to-date. The organization's IoT suppliers make available user guides or manuals for the IoT products and/or services they provide, and they have plans in place for delivering IoT security and privacy training to IoT systems and/or software engineers.

The informative references for this IoTSRM2 control are [28,30]; [40]: 41, 43; [45]; [46]: TRN-01, TRN-02; [50]: 2.4.12.11, 2.4.12.12; [51]: Principle 2: Key concept 7; [53]: 4.2, 4.2.3, 4.2.6; [54]; [55]: OP-19, OP-20, OP-21, OP-23; [56]; [57]: GP 21, GP 27; [58,60].

IoT security incident response plan (GV.D.5): An IoT security incident response plan is documented, formally approved, periodically reviewed, up-to-date, readily available to staff, and involves relevant outside parties. This plan is aligned with and part of wider cybersecurity incident response and crisis management plans which are regularly reviewed, tested, and updated. The organization's IoT suppliers have and maintain cybersecurity incident response plans which incorporate IoT security considerations and shared responsibilities with IoT adopters, and they communicate these plans to IoT adopters.

The informative references for this IoTSRM2 control are [28]; [40]: 40; [44,45]; [46]: IMT-02; [47,48]; [50]: 2.4.3.8, 2.4.3.21; [55]: OP-10, OP-11, OP-12; [57]: GP 22, GP 23; [60].

IoT vulnerability management plan (GV.D.6): An IoT vulnerability management plan, which is aligned with and supports the overall vulnerability management program, is established, documented, formally approved, periodically reviewed, and up-to-date. The organization's IoT suppliers have and maintain vulnerability management plans for keeping internal infrastructure and applications updated, and vulnerability disclosure plans to enable third party vulnerability reporting, disclosure of vulnerabilities, and release of security advisories and patches for the IoT systems they provide.

The informative references for this IoTSRM2 control are [28]; [40]: 2, 9; [46]: OPA-01, VLN-01; [47,49]; [50]: 2.4.3.7, 2.4.3.9, 2.4.13.5; [51]: Principle 5: Key Concept 17; [52]; [53]: 4.2.4; [54]; [55]: OP-14, OP-15, OP-16, OP-18; [56]; [57]: GP 24, GP 26; [58–60].

IoT End-of-Life plan (GV.D.7): An IoT End-of-Life plan, which is aligned with and part of the organization's decommissioning strategy, is defined, documented, approved by board committees and/or C-suite executives, periodically reviewed, up-to-date, and well communicated across the organization. The organization's IoT suppliers have and maintain End-of-Life policies and communicate their sunsetting plans, practices, and implications to IoT adopters.

The informative references for this IoTSRM2 control are [28]; [40]: 33, 34; [46]: EOL-01; [47,49]; [53]: 3.4, 4.2.2, 4.2.5; [55]: OP-01; [56,58,59].

Then, for each IoTSRM2 objective of the "Governance" domain, Table 6 provides the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 controls with their adjusted weights. These IoTSRM2 controls are prioritized within each IoTSRM2 objective. Hence, for "Security related policies", "Structures and responsibilities", "Regulatory requirements", and "Governance and risk management plans", the most important IoTSRM2 controls based on adjusted weights are "IoT security policy", "IoT security governance structures and responsibilities", "Cybersecurity regulatory framework", and "IoT security and privacy controls management plan", respectively.

Risk Assessment (RA)

The "Risk Assessment" domain of IoTSRM2 consists of the following four objectives:

- Vulnerability discovery (RA.A): Determine whether IoT vulnerabilities are identified and documented;
- Threat identification (RA.B): Determine whether IoT threats are identified and documented;
- Risk analysis (RA.C): Determine whether IoT risks are identified and analyzed;
- Risk responses (RA.D): Determine whether IoT risk responses are identified and prioritized.

Vulnerability discovery (RA.A)

The "Vulnerability discovery" objective has two IoTSRM2 controls.

Disclosure-based IoT vulnerability discovery (RA.A.1): Cybersecurity and privacy vulnerabilities across the organization's IoT assets are continuously identified and documented from multiple external sources. The activities of identifying IoT vulnerabilities from external sources are coordinated as part of the organization's cybersecurity risk assessment process. The organization's IoT suppliers use information sharing platforms for finding vulnerability information and leverage their vulnerability disclosure policy and mechanisms to incentivize third-party vulnerability reporting and to release timely security advisories for the identified vulnerabilities in the IoT products and/or services they provide.

The informative references for this IoTSRM2 control are [28,30]; [40]: 9; [41,42]; [46]: SDV-05; [47,49]; [50]: 2.4.3.7, 2.4.3.9; [51]: Principle 5: Key concept 18; [54,59–61].

Assessment-based IoT vulnerability discovery (RA.A.2): The attack surface of the organization's IoT footprint across its entire system lifecycle is continuously or periodically identified and documented using a blend of various well-structured assessment processes which leverage effective cybersecurity methodologies and solutions. The activities of identifying IoT vulnerabilities and control weaknesses are coordinated as part of the organization's cybersecurity risk assessment process. The organization's IoT suppliers perform and document continuous or periodic assessments of their cybersecurity postures and of the vulnerabilities relating to the IoT products and/or services they provide, in order to achieve ongoing vulnerability monitoring and cybersecurity improvement.

The informative references for this IoTSRM2 control are [28,30]; [40]: 8, 10, 12, 44; [44]; [46]: GVN-03, PRV-02, PRV-04, RSM-02, SOP-02, TMM-01, TMM-02, TMM-04, VLN-01; [47,48]; [50]: 2.4.10.9, 2.4.13.5; [51]: Principle 2: Key concept 4, Principle 2: Key concept 5, Principle 2: Key concept 6, Principle 5: Key concept 21; [52,54]; [55]: PS-09, PS-19, PS-21, OP-04, OP-17, TM-10, TM-14, TM-15; [56]; [57]: GP 2, GP 8, GP 11, GP 19, GP 30; [58–60].

Threat identification (RA.B)

The "Threat identification" objective has two IoTSRM2 controls.

Intelligence-driven IoT threat identification (RA.B.1): IoT threats are continuously identified, centralized, and documented from multiple external threat sharing sources. The activities of identifying IoT threats from external sources are coordinated as part of the organization's cybersecurity risk assessment process and in line with cyber threat intelligence program. The organization's IoT suppliers continuously engage in cyber threat information sharing, employ cyber threat intelligence for acquiring insights into the latest cyber threats and data breaches, and leverage an effective vulnerability disclosure program for identifying cyber threats to the IoT products and/or services they provide and releasing security advisories.

The informative references for this IoTSRM2 control are [28,30]; [40]: 9; [46]: TMM-03; [51]: Principle 5: Key concept 18; [54]; [55]: PS-22, OP-23; [59,60].

Assessment-based IoT threat identification (RA.B.2): Cyber threats are continuously or periodically identified, profiled, and documented at an appropriate level of detail throughout the organization's IoT system lifecycle using a blend of conventional and cyber kill chain-based assessments which employ appropriate task automation and effective cybersecurity intelligence and analytics solutions. The activities of identifying IoT threats are coordinated as part of the organization's cybersecurity risk assessment process. The organization's IoT suppliers conduct and document continuous or periodic cybersecurity current state assessments and continuously identify and monitor the cyber threats relevant to the IoT products and/or services they provide.

The informative references for this IoTSRM2 control are [28]; [40]: 8, 44; [44]; [46]: PRV-02, PRV-04, RSM-02, TMM-01, SOP-02, VLN-01; [47,48]; [50]: 2.4.10.9; [51]: Principle 2: Key concept 4, Principle 2: Key concept 5, Principle 2: Key concept 6; [52,54]; [55]: PS-09, PS-19, PS-21, PS-23, OP-17, TM-10, TM-14, TM-15; [56]; [57]: GP 11, GP 13, GP 19; [59,60].

Risk analysis (RA.C)

The "Risk analysis" objective has one IoTSRM2 control, namely "IoT risk identification and analysis" control.

IoT risk identification and analysis (RA.C.1): IoT risks are regularly identified, analyzed, and recorded through thoughtful and methodical IoT risk assessments which entail estimation of likelihoods and business impacts of IoT risks using both quantitative and qualitative methodologies. The activities of identifying, analyzing, and recording IoT risks are performed as part of the organization's cybersecurity risk assessment process. The organization’s IoT suppliers perform periodic cybersecurity risk assessments throughout their organization and continuously monitor and assess the risks of confidentiality, integrity, availability, and safety of the IoT products and/or services they provide being compromised.

The informative references for this IoTSRM2 control are [28]; [40]: 8, 9, 44; [41,44]; [46]: PRV-02, PRV-04, RSM-02, SOP-01, SOP-02, TMM-01, VLN-01; [48]; [50]: 2.4.10.9; [51]: Principle 2: Key concept 4, Principle 2: Key concept 5, Principle 2: Key concept 6, Principle 5: Key concept 18; [54]; [55]: PS-09, PS-19, PS-21, PS-23, TM-10, TM-14, TM-15; [56]; [57]: GP 11, GP 19; [59,60].

Risk responses (RA.D)

The “Risk responses” objective has one IoTSRM2 control, namely “Cybersecurity risk register and IoT risk responses” control.

Cybersecurity risk register and IoT risk responses (RA.D.1): Cybersecurity, privacy, and safety risks relevant for the organization’s IoT infrastructure and associated risk responses are recorded, prioritized, centralized, and tracked as part of a formally approved, periodically reviewed, and up-to-date cybersecurity risk register and in line with the overarching cybersecurity risk management strategy. This cybersecurity risk register is aligned with and part of the broader enterprise cybersecurity risk register. The organization’s IoT suppliers have and maintain comprehensive cybersecurity risk registers to adequately manage the cybersecurity and privacy risks to the IoT products and/or services they provide.

The informative references for this IoTSRM2 control are [28]; [40]: 9; [44]; [46]: PRV-02, PRV-04, RSM-02, SOP-01, TMM-01, VLN-01; [48]; [50]: 2.4.10.9; [54]; [55]: PS-09, PS-19, PS-21, TM-14; [57]: GP 11, GP 19; [59,60].

Then, for each IoTSRM2 objective of the “Risk Assessment” domain, Table 7 provides the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 controls with their adjusted weights. These IoTSRM2 controls are prioritized within each IoTSRM2 objective. Hence, for “Vulnerability discovery”, “Threat identification”, “Risk analysis”, and “Risk responses”, the most important IoTSRM2 controls based on adjusted weights are “Assessment-based IoT vulnerability discovery”, “Assessment-based IoT threat identification”, “IoT risk identification and analysis”, and “Cybersecurity risk register and IoT risk responses”, respectively.

Risk Management Strategy (RM)

The “Risk Management Strategy” domain of IoTSRM2 consists of the following two objectives:

- Risk appetite and tolerances (RM.A): Determine whether IoT security risk appetite and tolerances are determined and clearly expressed;
- Context-informed risk tolerances (RM.B): Determine whether IoT security risk tolerances are informed by the entity’s role in critical infrastructure and sector specific risk analysis.

Risk appetite and tolerances (RM.A)

The “Risk appetite and tolerances” objective has one IoTSRM2 control, namely “IoT security risk appetite and tolerances” control.

IoT security risk appetite and tolerances (RM.A.1): IoT security risk appetite and associated range of risk tolerances are clearly articulated and documented as part of board approved, periodically reviewed, and up-to-date IoT security risk appetite and tolerance statements. These statements are defined based on IoT security and cybersecurity risk management best practices, are in line with the organization’s appetites and tolerances for cybersecurity and privacy risks, support the objectives of the organization’s risk management strategy, and trigger re-assessments of cybersecurity and privacy risk appetites and tolerances. The organization’s IoT suppliers clearly articulate and document their appetites and associated tolerances for cybersecurity, privacy, and IoT security risks, and communicate their risk appetite and tolerance statements to IoT adopters.

The informative references for this IoTSRM2 control are [46]: RSM-01; [48]; [50]: 2.4.3.4; [52,54]; [55]: PS-18.

Context-informed risk tolerances (RM.B)

The "Context-informed risk tolerances" objective has one IoTSRM2 control, namely "Context-informed IoT security risk tolerances" control.

Context-informed IoT security risk tolerances (RM.B.1): IoT security risk tolerance determination leverages a clear understanding of the criticality of the organization's infrastructure and the associated interdependencies with critical infrastructure, along with the organization's awareness of the risk profile for the sector in which it operates. These IoT risk tolerances are aligned with the organization's appetites for IoT security, privacy, and cybersecurity risks. The organization's IoT suppliers know their roles in critical infrastructure, clearly articulate and document their tolerances for cybersecurity, privacy, and IoT security risks, and communicate their risk appetite and tolerance statements to IoT adopters.

The informative references for this IoTSRM2 control are [46]: RSM-01; [48]; [50]: 2.4.3.4; [52]; [53]: 4.2.1; [55]: PS-18.

Then, for each IoTSRM2 objective of the "Risk Management Strategy" domain, Table 8 provides the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 control with its adjusted weight. These IoTSRM2 controls are already prioritized within each IoTSRM2 objective given that there is only one control for each objective, and in effect the adjusted weight of each IoTSRM2 control is the same as the weight of the associated IoTSRM2 objective.

Supply Chain Risk Management (SC)

The "Supply Chain Risk Management" domain of IoTSRM2 consists of the following two objectives:

- Supplier assessment (SC.A): Determine whether IoT suppliers across supply chain tiers are identified, risk assessed, and prioritized following the IoT supply chain risk management plan;
- Supplier contract management (SC.B): Determine whether IoT supplier contract requirements are defined following the IoT supplier contract management plan.

Supplier assessment (SC.A)

The "Supplier assessment" objective has two IoTSRM2 controls.

IoT supply chain risk management plan (SC.A.1): An organization-wide IoT supply chain risk management plan, which is aligned with IoT security policy and part of broader cyber supply chain risk management program, is documented, formally approved, periodically reviewed, and up-to-date. The organization's IoT suppliers have and maintain cyber supply chain risk management plans to effectively address cyber supply chain risks across their whole IoT supply chains.

The informative references for this IoTSRM2 control are [28]; [40]: 12; [46]: SDV-15; [47,48]; [50]: 2.4.3.6; [55]: OP-26, TM-07; [56,58,60].

IoT supply chain risk assessment (SC.A.2): IoT suppliers across supply chain tiers are identified and tracked throughout the entire supplier relationship lifecycle, their criticality to the business is determined, and IoT supply chain risks are regularly assessed and recorded as part of the board-approved, periodically reviewed, and up-to-date cybersecurity risk register. The IoT supply chain risk assessment follows the IoT supply chain risk management plan. The organization's IoT suppliers continuously or regularly assess cybersecurity and privacy supply chain risks through a combination of supplier assessments (e.g., penetration tests, site visits), document findings incorporating IoT supply chain risk exposures, and disclose cybersecurity-related supply chain risk assessment findings to IoT adopters.

The informative references for this IoTSRM2 control are [40]: 11; [43–45]; [46]: RSM-02; [48]; [53]: 4.2.3; [54]; [55]: PS-19, TM-10; [56,59,60].

Supplier contract management (SC.B)

The "Supplier contract management" objective has two IoTSRM2 controls.

IoT supplier contract management plan (SC.B.1): An organization-wide IoT supplier contract management plan, which is aligned with and part of a wider contract management plan, is documented, formally approved, periodically reviewed, and up-to-date. This plan is in line with the organization's IoT security and privacy controls framework, cybersecurity regulatory framework, and IoT security policy, and it is part of the broader cyber supply chain risk management program. The organization's IoT suppliers have and maintain robust supplier contract management plans for ensuring trusted supplier relationships throughout the entire contract lifecycle and disclose relevant supply chain changes to IoT adopters.

The informative references for this IoTSRM2 control are [28]; [40]: 1, 21, 29; [41,44]; [46]: OPA-05, RMT-01; [48]; [50]: 2.4.5.36; [51]: Principle 5: Key concept 20; [53]: 4.2.1, 4.2.3, 4.2.4; [55]: OP-05, OP-27, TM-30; [56]; [57]: GP 23; [58].

IoT trustworthiness requirements (SC.B.2): Cybersecurity, privacy, safety, reliability, and resiliency requirements for the organization's IoT supplier contracts are established, documented, formally approved, periodically reviewed, and up-to-date. These requirements are defined based on applicable IoT regulations, IoT security best practices, and the organization's IoT security policy as part of the IoT supplier contract management plan. The organization's IoT suppliers provide up-to-date cybersecurity bills of materials (CBOMs) to IoT adopters for the IoT products they acquire, hold original equipment manufacturers (OEMs) accountable to ensure trust down the supply chain, and have IoT supplier contracts that incorporate cybersecurity, privacy, safety, reliability, and resiliency requirements which provide appropriate levels of detail, clarity, trustworthiness, and service targets, to enable IoT supply chain of trust.

The informative references for this IoTSRM2 control are [28,30]; [40]: 3, 4, 12, 22, 24, 26, 28, 31, 36, 44; [46]: CLS-04, GVN-02, RMT-02; [48]; [51]: Principle 2: Key concept 3; [54]; [55]: PS-06, OP-01, OP-02, OP-03, OP-26, TM-08, TM-09; [57]: GP 30; [58,59].

Then, for each IoTSRM2 objective of the "Supply Chain Risk Management" domain, Table 9 provides the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 controls with their adjusted weights. These IoTSRM2 controls are prioritized within each IoTSRM2 objective. Hence, for "Supplier assessment" and "Supplier contract management", the most important IoTSRM2 controls based on adjusted weights are "IoT supply chain risk management plan" and "IoT trustworthiness requirements", respectively.

3.2. Evaluation of Selected Informative References of IoTSRM2

This subsection provides a critical evaluation of selected informative references of IoTSRM2 based on their percentage-wise linkage to IoTSRM2. Thus, from the 25 informative references of IoTSRM2, this evaluation focuses exclusively on the informative references that are considered the most relevant to IoT security risk management strategy based on the fulfilment of the two inclusion criteria and two conditions (see Section 2.2). Thus, the informative references that are selected in-scope for our critical evaluation are [40,46,50,51,53,55,57].

First, the selected informative references are critically evaluated relative to their percentage-wise linkage to the IoTSRM2 domains. Then, they are critically evaluated relative to their percentage-wise linkage to the entire IoTSRM2. Figure 4 shows, for each selected informative reference of IoTSRM2, the following details:

- for each IoTSRM2 domain, the percentage of all IoT security requirements applicable to the IoTSRM2 domain in question of each selected informative reference of the total number of IoT security requirements applicable to the IoTSRM2 domain in question of all 25 informative references;
- for the entire IoTSRM2, the percentage of all IoT security requirements applicable to IoTSRM2 of each selected informative reference of the total number of IoT security requirements applicable to IoTSRM2 of all 25 informative references.

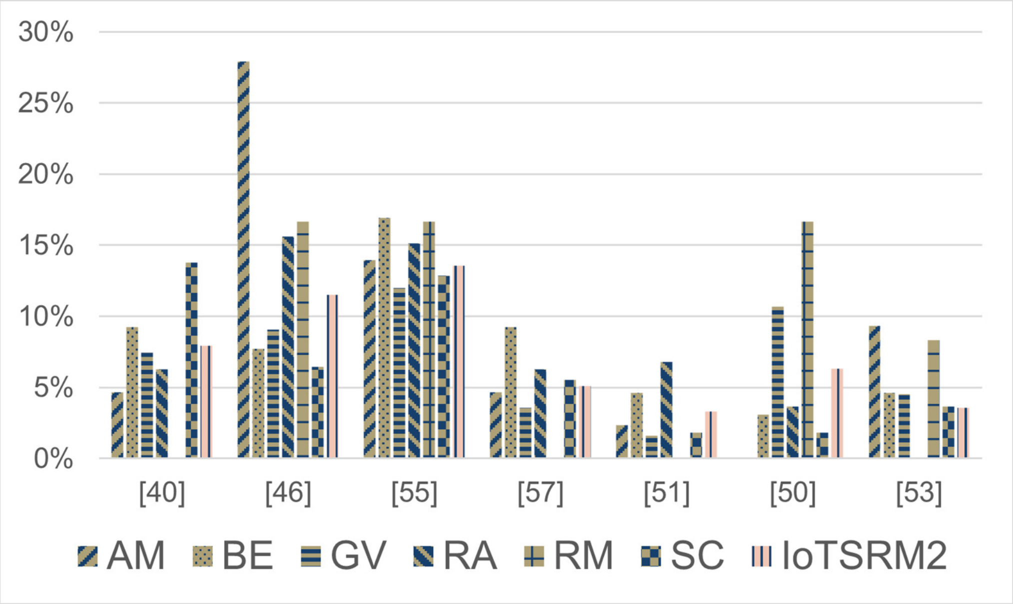

Figure 4. Percentage-wise evaluation of selected informative references of IoTSRM2.

With respect to the percentage-wise linkage of the selected informative references to each IoTSRM2 domain, while Refs. [40,46,50,55] each resulted as the most linked to some of the IoTSRM2 domains, Refs. [40,50,51,53,57] each resulted as the least linked to some of the IoTSRM2 domains. First, about [40], from the selected references, it resulted in being the most linked to the "Supply Chain Risk Management" domain, and it resulted in being the least linked to the "Risk Management Strategy" domain. Second, with respect to [46], from the selected references, it resulted in being the most linked to the "Asset Management", "Risk Assessment", and "Risk Management Strategy" domains. Third, regarding [55], from the selected references, it resulted in being the most linked to the "Business Environment", "Governance", and "Risk Management Strategy" domains. Fourth, about [57], from the selected references, it resulted in being the least linked to the "Risk Management Strategy" domain. Then, about [51], from the selected references, it resulted in being the least linked to the "Governance", "Risk Management Strategy", and "Supply Chain Risk Management" domains. Next, with regard to [50], from the selected references, it resulted in being the most linked to the "Risk Management Strategy", and it resulted in being the least linked to the "Asset Management", "Business Environment", and "Supply Chain Risk Management" domains. In addition, with regard to [53], from the selected references, it resulted in being the least linked to the "Risk Assessment" domain.

With respect to the percentage-wise linkage of the selected informative references to the entire IoTSRM2, Refs. [40,46,55] resulted in being the top three most linked to IoTSRM2, in that order, whereas Refs. [51,53,57] resulted in being the top three least linked to IoTSRM2, in that order. The logic behind these outputs is very much driven by the "Governance", "Risk Assessment", and "Supply Chain Risk Management" domains of IoTSRM2 given that the number of in-scope IoT security requirements mapped against them amount to around 84% of the total number of in-scope IoT security requirements linked to IoTSRM2.

Hence, with respect to [55], its very high percentage score is primarily because, from the selected informative references, it is the most linked to the "Governance" domain of IoTSRM2, which has the greatest number of in-scope IoT security requirements mapped to it among the IoTSRM2 domains (i.e., 42%), and it is the second most linked to both the "Risk Assessment" and "Supply Chain Risk Management" domains of IoTSRM2, which are the next in line in terms of their corresponding numbers of mapped in-scope IoT security requirements, namely 26% and 15%, respectively. About [46], its high percentage score is mainly because, from the selected informative references, it is the most linked to the

"Risk Assessment", and it is the third most linked to both the "Governance" and "Supply Chain Risk Management" domains of IoTSRM2. Regarding [40], its fairly high percentage score is mostly because, from the selected informative references, it is the most linked to the "Supply Chain Risk Management", and it is the fourth most linked to both the "Governance" and "Risk Assessment" domains of IoTSRM2.

Then, with respect to [51], its very low percentage score is mainly because, from the selected informative references, it is the least linked to the "Governance" domain, and the same as [50], it is the least linked to the "Supply Chain Risk Management" domain. With regard to [53], its low percentage score is mainly because, from the selected informative references, it is the third least linked to both the "Governance" and "Supply Chain Risk Management" domains, and it is the least linked to the "Risk Assessment" domain of IoTSRM2. As for [57], its fairly low percentage score is majorly because, from the selected informative references, it is the second least linked to the "Governance" domain, and the same as [40], it is the third least linked to the "Risk Assessment" domain of IoTSRM2.

Thus, the resulting outcomes reflect the inclusion criteria of the selected informative references (see Section 2.2). In addition, it is worth noting that [55] has the strongest links to IoTSRM2 among all 25 informative references, and [51] is the least linked to IoTSRM2 among the selected informative references.

Furthermore, Figure 5 outlines the focus of each of the selected informative references from a strategic perspective, relative to each of the IoTSRM2 domains. This is based on the number of in-scope IoT security requirements corresponding to each selected informative reference for the IoTSRM2 domain in question. First, Ref. [40], the same as Ref. [55], is the most focused on the "Governance" domain, and it is the least focused on the "Risk Management Strategy" domain. Next, Ref. [46], the same as Refs. [51,57], is the most focused on the "Risk Assessment" domain, and it is the least focused on the "Risk Management Strategy" domain. Then, Ref. [50] is the most focused on the "Governance" domain, and it is the least focused on the "Asset Management" domain. In addition, Ref. [53] is the most focused on the "Governance" domain, and it is the least focused on the "Risk Assessment" domain. Thus, it is worth noting that the majority of the selected informative references are the most focused on the "Governance" domain, and they are the least focused on the "Risk Management Strategy" domain.

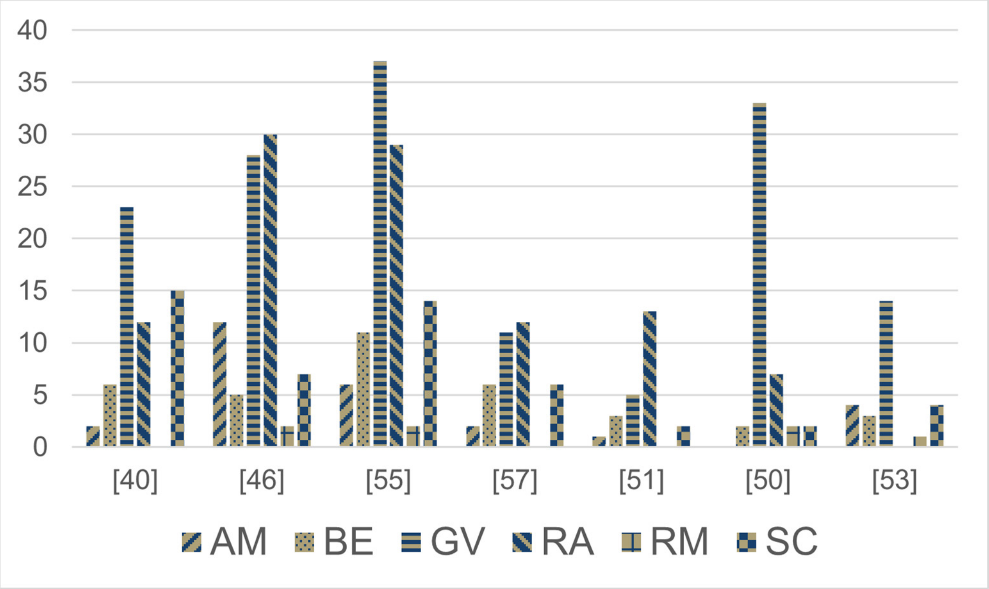

Figure 5. Evaluation of selected informative references of IoTSRM2.

4. Related Work

A sizeable number of best practices and academic papers has been published on IoT security; however, the majority of these are more technical in nature (e.g., [26,30,43,74,75]). Moreover, at the time of writing, there is no research article nor best practice to exclusively focus on IoT security risk management strategy. In this context, Lee [12] proposed a four-layer IoT cyber risk management framework, which includes the IoT cyber ecosystem layer, the IoT cyber infrastructure layer, the IoT cyber risk assessment layer, and the IoT cyber performance layer. Nevertheless, the IoT cyber risk management framework proposed by Lee [12] outlines the framework's layers instead of providing IoT security controls/requirements, is not exclusively focused on IoT security risk management strategy, and it is based on cybersecurity risk management practices rather than IoT security best practices. Thus, compared with the work performed by Lee [12], our proposed IoTSRM2 is exclusively focused on IoT security risk management strategy, is based on 25 selected IoT security best practices, and provides expected IoT security risk management controls, among others.

Moreover, some of the previous studies concentrated on the state of the art of IoT security best practices (i.e., [18,24]) or on delivering an overview and catalogue of key IoT security initiatives [76]. For instance, ECSO [24], Garcia-Morchon et al. [18], and CSA Singapore along with MEAC of the Netherlands [76] provided overviews around IoT security best practices, but they did not clearly link the applicability of each best practice to a specific group of target audience (i.e., adopters, suppliers, manufacturers, general) nor did they classify each best practice based on type (i.e., codes of practice, standards, guidelines, frameworks). Hence, as part of Section 2.1, besides providing an overview of some of the most renowned IoT security best practices, this article proposed a taxonomic hierarchy for classifying best practices based on their applicability and type, and this taxonomy is used for outlining the 25 selected IoT security best practices.

Furthermore, the available documentation around the 25 selected IoT security best practices was used to provide the overview of IoT security best practices, our proposed IoTSRM2, and the analysis of IoTSRM2's related work from this section (see Table 10).

Then, with respect to the analysis of IoTSRM2's related work, Table 10 shows the IoTSRM2 together with the 25 selected IoT security best practices mapped against the proposed evaluation criteria and the extent of applicability to each evaluation criterion. With respect to the proposed evaluation criteria, eight evaluation criteria were formulated based on our proposed methodology for developing the IoTSRM2 (see Section 2.2). In addition, with respect to the extent of applicability, three types of applicability were considered relevant to indicate differences and/or similarities between the proposed IoTSRM2 and the in-scope research works for this evaluation.

Following Table 10, this section presents the evaluation of IoTSRM2 and the 25 selected IoT security best practices for each evaluation criterion.

E1: Focus on strategic IoT security practices over technical IoT security practices

Our proposed IoTSRM2 is exclusively focused on IoT security risk management strategy. In addition, from the 25 selected IoT security best practices, seven of them focused on strategic IoT security activities (i.e., [40,51–54,57,59]), ten of them had a partial focus on strategic IoT security activities (i.e., [28,42,44,45,48,55,56,58,60,61]), while the remaining ones focused on technical IoT security activities (i.e., [26,30,41,43,46,47,49,50]).

Regarding the seven selected IoT security best practices that focused on strategic IoT security activities, AgeLight LLC [40], DHS [59], NEMA [52], and OTA [54] provided strategic IoT security principles, ENISA [57] provided strategic guidelines specifically focused on procurement in hospitals, IoTAC [51] provided basic strategic guidance for providers and users of IoT devices, systems, and services across industries, and NIST [53] provided premarket and postmarket cybersecurity activities with a strategic focus for IoT device manufacturers. Similar to these seven selected IoT security best practices which provided IoT security requirements with a strategic focus, our proposed IoTSRM2 provides domains, objectives, and controls focused on strategic IoT security practices. Compared with the seven selected IoT security best practices which were not exclusively focused on IoT security risk management strategy, this article proposes a reference model for IoT security risk management strategy (i.e., IoTSRM2) applicable to IoT adopters from any sector.

Table 10. IoTSRM2 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, But Not Fully**	**The "as-is" Evaluation Criterion Does Not Apply**
E1: Focus on strategic IoT security practices over technical IoT security practices	[40,51–54,57,59], IoTSRM2	[28,42,44,45,48,55,56,58,60,61]	[26,30,41,43,46,47,49,50]
E2: Methodology for developing the recommended IoT security requirements/controls is clearly described	[26,28,41,55–58], IoTSRM2	[30,40,43,61]	[42,44–54,59,60]
E3: Mapping of IoT security requirements/controls to NIST CSF's Categories and Subcategories	IoTSRM2, but none of the 25 selected IoT security best practices	[28,40]	All 25 selected IoT security best practices except [28,40]
E4: Clearly indicate for each IoT security requirement/control expected IoT security actions/activities from IoT suppliers of the target audience	IoTSRM2, but none of the 25 selected IoT security best practices	[28,43,44,48,51,55–59]	[26,30,40–42,45–47,49,50,52–54,60,61]
E5: Provides integration points with the cybersecurity program as part of each IoT security requirement/control	IoTSRM2, but none of the 25 selected IoT security best practices	[45,55–57]	All 25 selected IoT security best practices except [45,55–57]
E6: Mapping of relevant IoT security best practices with unique identifiers for selected best practices to each recommended IoT security requirement/control	[26,61], IoTSRM2	[28,40,46,50–53,55,56,58,60]	[30,41–45,47–49,54,57,59]
E7: Prioritization of the recommended IoT security requirements/controls	[42,49,61], IoTSRM2	[40,47,50,54]	All 25 selected IoT security best practices except [40,42,47,49,50,54,61]
E8: Provides statistics for the mapping of selected informative references	[61], IoTSRM2	None of the 25 selected IoT security best practices	All 25 selected IoT security best practices except [61]

Furthermore, from the perspective of the extent of applicability to this evaluation criterion, compared with the ten selected IoT security best practices (i.e., [28,42,44,45,48,55,56,58,60,61]), which, besides the strategic IoT security practices focused on some technical IoT security practices, our proposed IoTSRM2 exclusively focused on strategic IoT security practices.

E2: Methodology for developing the recommended IoT security requirements/controls is clearly described

Our proposed methodology for developing IoTSRM2 controls is clearly described. In addition, from the 25 selected IoT security best practices, seven of them clearly described the methodology used for developing the recommended IoT security requirements (i.e., [26,28,41,55–58]), four of them partially described their methodology (i.e., [30,40,43,61]), while the remaining ones have not described their methodology (i.e., [42,44–54,59,60]).

Regarding the seven selected IoT security best practices that clearly described their methodologies, AIOTI [41] provided details about the aspects discussed as part of the four sessions workshop, CSDE [26] developed the IoT security requirements by identifying common IoT security device capabilities from Convening the Conveners (C2) organizations, ENISA [57] analyzed the data received through a series of interviews for recommending the IoT security requirements, and the other four IoT security best practices of ENISA (i.e., [28,55,56,58]) used the ENISA's five-step methodology involving both desktop research and interviews. Compared with the high-level five-step methodology from ENISA (i.e., [28,55,56,58]), our proposed three-phased methodology for developing the IoTSRM2 consists of nine steps, and it is much more comprehensive as it provides a far greater level of detail with respect to the steps involved. Even though our proposed methodology from this article has different objectives than the studies conducted by ENISA [28,55,56,58], similar to the methodology of ENISA (i.e., [28,55,56,58]) which included scope definition, desktop research, and analysis and development tasks, among others, our proposed methodology for developing the IoTSRM2 includes several steps related to scoping, analysis, and creation phases that involve extensive research work. In addition, in contrast to the research works performed by AIOTI [41], CSDE [26], and ENISA [57] which are limited to workshops, surveys, and interviews, respectively, our proposed methodology from this article is based on selected IoT security best practices.

Furthermore, from the perspective of the extent of applicability to this evaluation criterion, our proposed methodology for developing the IoTSRM2 differentiates from the methodologies provided by AgeLight LLC [40], BITAG [43], DCMS [61], and ETSI [30], as it is much more detailed than the ones of the four selected IoT security best practices which offered limited details. Thus, first, AgeLight LLC [40,77] developed the recommended IoT security requirements based on seven pre-established guiding tenets and dozens of industry and governmental efforts. AgeLight LLC [40,77] provided merely a couple of the efforts on which its methodology was built on rather than providing all sources and did not clearly outline the ways in which these efforts were used to develop the recommended IoT security requirements. Second, BITAG [43] did not outline the scenarios used by the Technical Working Group (TWG) representatives for achieving consensus around the recommended IoT security requirements through the BITAG's consensus process. Then, DCMS [27,61] described the methodology for developing the IoT security requirements half-way as it provided only the methodology for mapping of recommendations and guidance rather than the entire methodology used [27]. As for ETSI [30], it mentioned that its methodology relied solely on a documentary review of published standards, recommendations, and guidance on IoT security and privacy and provided the sources used to develop the recommended IoT security requirements, but it did not explain how these sources were put together and processed.

E3: Mapping of IoT security requirements/controls to NIST CSF's Categories and Subcategories

As per Table 10 above, none of the 25 selected IoT security best practices provided a complete mapping of their recommended IoT security requirements to the NIST CSF's Categories and Subcategories. However, AgeLight LLC [40] and ENISA [28] provided a partial mapping of their IoT security requirements to the NIST CSF, and this is because their IoT security requirements were not mapped against the NIST CSF's Categories and Subcategories. In contrast to the 25 selected IoT security best practices, our proposed IoTSRM2 provides the IoTSRM2 domains based on the Categories of NIST CSF Identify Function, the IoTSRM2 objectives based on in-scope NIST CSF Subcategories, and the mapping of in-scope NIST CSF Subcategories to the IoTSRM2 objectives (see Sections 2.2 and 3.1).

E4: Clearly indicate for each IoT security requirement/control expected IoT security actions/activities from IoT suppliers of the target audience

None of the 25 selected IoT security best practices clearly indicated for each of their recommended IoT security requirements expected IoT security actions/activities from the IoT suppliers of the target audience. However, ten of these, namely BITAG [43], CSA [44], DHS [59], ENISA [28,55–58], IIC [48], and IoTAC [51], indicated for some IoT security requirements expected IoT security actions/activities from IoT suppliers of the target audience. In contrast to the 25 selected IoT security best practices, our proposed IoTSRM2 provides for each IoT security control IoT security related activities/actions of IoT suppliers that govern their postmarket activities and that IoT adopters should expect from them.

E5: Provides integration points with the cybersecurity program as part of each IoT security requirement/control

None of the 25 selected IoT security best practices provided integration points with the cybersecurity program as part of each IoT security requirement. CSA [45] and ENISA [55–57] provided for a few IoT security requirements integration points with the cybersecurity program. Compared with the 25 selected IoT security best practices, our proposed IoTSRM2 provides, for each IoT security control, integration points for the expected IoT security related activities/actions with the cybersecurity programs of IoT adopters.

E6: Mapping of relevant IoT security best practices with unique identifiers for selected best practices to each recommended IoT security requirement/control

Our proposed methodology for developing IoTSRM2 involves the mapping of the 25 selected IoT security best practices with unique identifiers for selected best practices to each IoTSRM2 control where applicable. In addition, from the 25 selected IoT security best practices, two of them provided the mapping of relevant IoT security best practices with unique identifiers for each recommended IoT security requirement (i.e., [26,61]), eleven of them partially provided this type of mapping (i.e., [28,40,46,50–53,55,56,58,60]), while the remaining ones have not provided this type of mapping (i.e., [30,41–45,47–49,54,57,59]).

Regarding the two selected IoT security best practices that provided the mapping of relevant IoT security best practices with unique identifiers to each recommended IoT security requirement, CSDE [26] provided under individual annexes the mapping of each IoT security requirement to the applicable requirement(s) of eleven best practices, and DCMS [61] provided in a separate document (i.e., [27]) the mapping of IoT security recommendations, guidance, and standards to each IoT security requirement of its code of practice. In this context, the mapping from IoTSRM2 is similar to the mappings provided by CSDE [26] and DCMS [27,61] which also provided the applicable informative references with associated unique identifiers (UIDs) of the in-scope IoT security requirements from various selected best practices. In addition, CSDE [26] and DCMS [27,61] provided the extracted text of those applicable IoT security requirements, but this level of detail is not targeted as part of the mapping for the proposed IoTSRM2 controls.

Furthermore, from the perspective of the extent of applicability to this evaluation criterion, compared with the mappings provided in the eleven selected IoT security best practices which offered incomplete or limited details, the mapping involved in the proposed methodology for developing the IoTSRM2 applies to all IoTSRM2 controls, and it is much more detailed. Thus, first, AgeLight LLC [40], and ENISA [28,55,56,58] provided this type of mapping without indicating the associated unique identifiers (UIDs) of the in-scope IoT security requirements from the relevant IoT security best practices. Second, IoTAC [51], NHTSA [60], and NIST [53] provided this type of mapping only for some of their IoT security requirements without indicating the associated unique identifiers (UIDs) of the in-scope IoT security requirements from the relevant IoT security best practices. Then, NEMA [52] provided this type of mapping only for some IoT security requirements with the associated unique identifiers (UIDs) of the in-scope IoT security requirements from the relevant IoT security best practices. Furthermore, IoTSF [50,69] provided the mapping of framework sections to ETSI TS 103 645 as part of the IoTSF Compliance Questionnaire [69], but this mapping was limited to framework sections rather than recommended IoT security requirements. In addition, CSA [46] provided the mapping of each IoT security requirement to the applicable control identifier(s) (IDs) of a best practice which is focused on cloud security (i.e., CSA Cloud Control Matrix—CCM) instead of IoT security.

E7: Prioritization of the recommended IoT security requirements/controls

Our proposed IoTSRM2 provides prioritized IoTSRM2 controls. In addition, from the 25 selected IoT security best practices, three of them provided the prioritization of the recommended IoT security requirements (i.e., [42,49,61]), four of them partially provided the prioritization of the recommended IoT security requirements (i.e., [40,47,50,54]), while the remaining ones did not provide this prioritization.

Regarding the three selected IoT security best practices that provided the prioritization of the recommended IoT security requirements, Commonwealth of Australia [42] and DCMS [61] prioritized their IoT security requirements recommending industry to prioritize the top three in the short-term and IEEE [49] prioritized its eleven IoT security requirements based on their relevance to IoT. Similar to these three IoT security best practices, our proposed IoTSRM2 provides prioritized IoTSRM2 controls. However, compared with these IoT security best practices which provided the prioritization of their IoT security requirements without describing how their prioritization resulted, our proposed methodology for developing the IoTSRM2 outlines the way in which the prioritization of IoTSRM2 controls for each IoTSRM2 objective was made. In addition, our proposed IoTSRM2 provides the prioritization of IoTSRM2 domains based on the number of IoTSRM2 objectives corresponding to each IoTSRM2 domain.

Furthermore, from the perspective of the extent of applicability to this evaluation criterion, compared with the prioritizations provided in the four IoT security best practices which covered only some IoT security requirements or offered limited details, the prioritization from IoTSRM2 covers all IoTSRM2 controls, and it is much more clearly outlined. Thus, first, AgeLight LLC [40] provided only the mechanism for prioritizing the IoT security requirements which consists of rating each security requirement based on company risk (i.e., user benefit, ecosystem impact, financial impact, hazardization, development effort and costs, regulatory risk). Second, GSM Association [47] prioritized only some IoT security requirements as "Critical", "High", "Medium", and "Low" instead of prioritizing all recommended IoT security requirements. Then, IoTSF [50] classified each IoT security requirement as "Mandatory" or "Advisory" rather than providing a comprehensive prioritization of its recommended IoT security requirements. Furthermore, OTA [54] classified each IoT security requirement as "Required (Must)" or "Recommended (Should)" instead of providing a comprehensive prioritization of its recommended IoT security requirements.

E8: Provides statistics for the mapping of selected informative references

Our proposed IoTSRM2 provides statistics for the mapping of selected informative references. In addition, from the 25 selected IoT security best practices, only DCMS [61] provided statistics for the mapping of informative references to their recommended best practices, while the remaining ones did not provide any statistics. Similar to DCMS [61] which provided the total number of IoT security recommendations mapped for each informative reference, our proposed IoTSRM2 provides, for each selected informative reference of IoTSRM2, the total number of unique in-scope IoT security requirements mapped to IoTSRM2 controls.

5. Conclusions and Future Work

This article proposed a reference model for IoT security risk management strategy that aims to support practitioners from organizations embracing IoT technologies to formulate or reframe their IoT security risk management strategies and achieve secure Internet of Things (IoT) adoption, and fellow researchers from academia that seek to explore the topic of IoT security risk management strategy as part of their research works.

First, this article outlined the key cybersecurity drivers, highlighted the need for successful adoption of new technologies, and provided the rationale for developing a reference model for IoT security risk management strategy.

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

Then, the article described our three-phased methodology for developing the proposed IoT security risk management strategy reference model (IoTSRM2), and it described the nine steps of the methodology and their associated outputs. Thus, first, the article described the three steps of the first phase (i.e., the scoping phase) which allowed the definition of methodology objectives and IoTSRM2 domains, among others. Afterwards, it described the three steps of the second phase (i.e., the analysis phase) which enabled, inter alia, the determination of the in-scope IoT security requirements from the 25 selected IoT security best practices, and of the IoTSRM2 controls. Next, it described the three steps of the third phase (i.e., the creation phase) which allowed, among others, the description and prioritization of the IoTSRM2 controls.

Subsequently, the article presented our proposed IoTSRM2. First, it provided an illustrative overview of the proposed IoTSRM2. Then, for each selected informative reference of IoTSRM2, it provided the total number of unique in-scope IoT security requirements mapped to IoTSRM2 controls. Next, for each IoTSRM2 domain, the article provided the IoTSRM2 objectives, and, for each IoTSRM2 objective, it described the IoTSRM2 controls in line with the target information granularity, and provided, among others, the prioritization of IoTSRM2 controls based on their adjusted weights.

Afterwards, this article provided a critical evaluation of the informative references of IoTSRM2 that were considered the most relevant to IoT security risk management strategy based on the fulfilment of pre-established inclusion criteria and conditions. The findings of this evaluation showed, among others, the selected informative references that are the top three most and least linked to the entire IoTSRM2.

Furthermore, this article outlined the related work. First, it highlighted the absence of research works that exclusively focus on IoT security risk management strategy. Then, it discussed the previous studies that focus on the state of the art or overviews of IoT security best practices, relative to IoTSRM2. Furthermore, to compare the proposed IoTSRM2 with related IoT security best practices, the article discussed the IoTSRM2 and the 25 selected IoT security best practices based on eight evaluation criteria and three types of applicability to each evaluation criterion.

Future work may include the undertaking of an IoTSRM2-based survey to analyze the gaps between the IoT security risk management strategies of selected organizations and the proposed IoTSRM2.

Author Contributions: Conceptualization, T.M.P.; methodology, T.M.P. and A.M.P.; reference model, 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.

Data Availability Statement: Data derived from public domain resources.

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

Appendix A

Table A1. Consolidated view of IoTSRM2 controls with informative references.

ID	IoTSRM2 Control	Informative References
AM.A.1	IoT hardware assets inventory	[30]; [40]: 12; [44,45]; [46]: ACT-01, ACT-03, ACT-04, ACT-05, GVN-01, OPA-01, TSP-02; [53]: 4.2.3, 4.2.6; [54]; [55]: PS-11, PS-12, PS-14; [57]: GP 28; [58,59]
AM.B.1	IoT software assets inventory	[40]: 12; [44]; [46]: ACT-01, ACT-03, ACT-05, GVN-01, TSP-02; [51]: Principle 2: Key concept 3; [53]: 4.2.3, 4.2.6; [54]; [55]: PS-11, PS-12, PS-14; [57]: GP 28; [58,59]
BE.A.1	Criticality and impact analysis	[28]; [40]: 12, 23, 44; [41]; [46]: GVN-02, SOP-01, SOP-02, TMM-04; [48]; [51]: Principle 2: Key concept 3, Principle 2: Key concept 5, Principle 5: Key concept 19; [53]: 4.2.1, 4.2.3, 4.2.6; [54]; [55]: PS-07, PS-08, PS-19, TM-10, TM-13; [56]; [57]: GP 7, GP 12; [58–60]
BE.B.1	Resiliency requirements	[28]; [40]: 12, 23, 44; [44,45]; [46]: BCN-01; [48]; [50]: 2.4.3.18, 2.4.3.23; [52,54]; [55]: OP-01, TM-09, TM-12, TM-15, TM-16, TM-17; [56]; [57]: GP 6, GP 17, GP 22, GP 23; [58–60].
GV.A.1	IoT security policy	[28,30]; [40]: 4, 5, 7; [41–44]; [46]: TSP-04; [47,48]; [50]: 2.4.3.4, 2.4.3.5, 2.4.3.6, 2.4.8.10; [51]: Principle 1: Key concept 1, Principle 1: Key concept 2; [55]: PS-18; [56]; [57]: GP 3, GP 5; [61]
GV.A.2	Privacy policy	[28,30]; [40]: 20, 22, 24, 25, 32, 35, 36; [42–44,47]; [50]: 2.4.12.5; [53]: 4.2.3; [54]; [55]: PS-06; [57]: GP 10; [61]
GV.A.3	Vulnerability disclosure policy	[28,30,42]; [46]: SDV-05; [49]; [50]: 2.4.3.11, 2.4.3.12, 2.4.3.13, 2.4.3.14, 2.4.3.16, 2.4.3.17; [53]: 4.2.6; [59–61]
GV.A.4	End-of-Life policy	[26,28,30]; [40]: 1, 21; [42]; [46]: EOL-01; [49]; [50]: 2.4.5.22, 2.4.5.35; [53]: 4.2.2, 4.2.5; [54,61]
GV.B.1	IoT security governance structures and responsibilities	[46]: GVN-01, UPD-01; [47]; [50]: 2.4.3.1, 2.4.3.2
GV.B.2	IoT security operations roles and responsibilities	[28,42,44]; [46]: BCN-01, IMT-02; [47]; [50]: 2.4.3.19, 2.4.3.20, 2.4.3.21, 2.4.12.12; [51]: Principle 5: Key concept 20; [53]: 4.2.1, 4.2.4; [55]: OP-08, OP-11; [56]; [57]: GP 1; [60,61]
GV.C.1	Cybersecurity regulatory framework	[28]; [40]: 31; [44]; [46]: CLS-04, GVN-02, RSM-01; [47,48,54]; [55]: PS-06, TM-07
GV.D.1	IoT security and privacy controls management plan	[28,30]; [40]: 5, 25, 30; [42,44,45]; [46]: BCN-01, RSM-01, SDV-15, UPD-03; [47,48]; [50]: 2.4.3.4, 2.4.12.6, 2.4.12.7, 2.4.16.1, 2.4.12.9, 2.4.12.10, 2.4.16.2; [55]: PS-01, PS-06, PS-16, PS-18, PS-20, PS-22, PS-24, OP-03, OP-06, OP-07, OP-09, OP-24, OP-25, TM-12, TM-14, TM-15, TM-16, TM-40, TM-57; [56]; [57]: GP 6; [58,61]
GV.D.2	IoT security budget plan	[28,56,60]
GV.D.3	IoT security measurement and reporting plan	[48]; [53]: 4.1; [56,58]
GV.D.4	IoT security training and awareness plan	[28,30]; [40]: 41, 43; [45]; [46]: TRN-01, TRN-02; [50]: 2.4.12.11, 2.4.12.12; [51]: Principle 2: Key concept 7; [53]: 4.2, 4.2.3, 4.2.6; [54]; [55]: OP-19, OP-20, OP-21, OP-23; [56]; [57]: GP 21, GP 27; [58,60]
GV.D.5	IoT security incident response plan	[28]; [40]: 40; [44,45]; [46]: IMT-02; [47,48]; [50]: 2.4.3.8, 2.4.3.21; [55]: OP-10, OP-11, OP-12; [57]: GP 22, GP 23; [60]
GV.D.6	IoT vulnerability management plan	[28]; [40]: 2, 9; [46]: OPA-01, VLN-01; [47,49]; [50]: 2.4.3.7, 2.4.3.9, 2.4.13.5; [51]: Principle 5: Key Concept 17; [52]; [53]: 4.2.4; [54]; [55]: OP-14, OP-15, OP-16, OP-18; [56]; [57]: GP 24, GP 26; [58–60]
GV.D.7	IoT End-of-Life plan	[28]; [40]: 33, 34; [46]: EOL-01; [47,49]; [53]: 3.4, 4.2.2, 4.2.5; [55]: OP-01; [56,58,59]

Table A1. *Cont.*

ID	IoTSRM2 Control	Informative References
RA.A.1	Disclosure-based IoT vulnerability discovery	[28,30]; [40]: 9; [41,42]; [46]: SDV-05; [47,49]; [50]: 2.4.3.7, 2.4.3.9; [51]: Principle 5: Key concept 18; [54,59–61]
RA.A.2	Assessment-based IoT vulnerability discovery	[28,30]; [40]: 8, 10, 12, 44; [44]; [46]: GVN-03, PRV-02, PRV-04, RSM-02, SOP-02, TMM-01, TMM-02, TMM-04, VLN-01; [47,48]; [50]: 2.4.10.9, 2.4.13.5; [51]: Principle 2: Key concept 4, Principle 2: Key concept 5, Principle 2: Key concept 6, Principle 5: Key concept 21; [52,54]; [55]: PS-09, PS-19, PS-21, OP-04, OP-17, TM-10, TM-14, TM-15; [56]; [57]: GP 2, GP 8, GP 11, GP 19, GP 30; [58–60]
RA.B.1	Intelligence-driven IoT threat identification	[28,30]; [40]: 9; [46]: TMM-03; [51]: Principle 5: Key concept 18; [54]; [55]: PS-22, OP-23; [59,60]
RA.B.2	Assessment-based IoT threat identification	[28]; [40]: 8, 44; [44]; [46]: PRV-02, PRV-04, RSM-02, TMM-01, SOP-02, VLN-01; [47,48]; [50]: 2.4.10.9; [51]: Principle 2: Key concept 4, Principle 2: Key concept 5, Principle 2: Key concept 6; [52,54]; [55]: PS-09, PS-19, PS-21, PS-23, OP-17, TM-10, TM-14, TM-15; [56]; [57]: GP 11, GP 13, GP 19; [59,60]
RA.C.1	IoT risk identification and analysis	[28]; [40]: 8, 9, 44; [41,44]; [46]: PRV-02, PRV-04, RSM-02, SOP-01, SOP-02, TMM-01, VLN-01; [48]; [50]: 2.4.10.9; [51]: Principle 2: Key concept 4, Principle 2: Key concept 5, Principle 2: Key concept 6, Principle 5: Key concept 18; [54]; [55]: PS-09, PS-19, PS-21, PS-23, TM-10, TM-14, TM-15; [56]; [57]: GP 11, GP 19; [59,60]
RA.D.1	Cybersecurity risk register and IoT risk responses	[28]; [40]: 9; [44]; [46]: PRV-02, PRV-04, RSM-02, SOP-01, TMM-01, VLN-01; [48]; [50]: 2.4.10.9; [54]; [55]: PS-09, PS-19, PS-21, TM-14; [57]: GP 11, GP 19; [59,60]
RM.A.1	IoT security risk appetite and tolerances	[46]: RSM-01; [48]; [50]: 2.4.3.4; [52,54]; [55]: PS-18
RM.B.1	Context-informed IoT security risk tolerances	[46]: RSM-01; [48]; [50]: 2.4.3.4; [52]; [53]: 4.2.1; [55]: PS-18
SC.A.1	IoT supply chain risk management plan	[28]; [40]: 12; [46]: SDV-15; [47,48]; [50]: 2.4.3.6; [55]: OP-26, TM-07; [56,58,60]
SC.A.2	IoT supply chain risk assessment	[40]: 11; [43–45]; [46]: RSM-02; [48]; [53]: 4.2.3; [54]; [55]: PS-19, TM-10; [56,59,60]
SC.B.1	IoT supplier contract management plan	[28]; [40]: 1, 21, 29; [41,44]; [46]: OPA-05, RMT-01; [48]; [50]: 2.4.5.36; [51]: Principle 5: Key concept 20; [53]: 4.2.1, 4.2.3, 4.2.4; [55]: OP-05, OP-27, TM-30; [56]; [57]: GP 23; [58]
SC.B.2	IoT trustworthiness requirements	[28,30]; [40]: 3, 4, 12, 22, 24, 26, 28, 31, 36, 44; [46]: CLS-04, GVN-02, RMT-02; [48]; [51]: Principle 2: Key concept 3; [54]; [55]: PS-06, OP-01, OP-02, OP-03, OP-26, TM-08, TM-09; [57]: GP 30; [58,59]

References

1. EY. How Does Security Evolve from Bolted on to Built-In? Bridging the Relationship Gap to Build a Business Aligned Security Program. EY Global Information Security Survey 2020. Available online: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-report.pdf (accessed on 2 April 2021).
2. 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.
3. 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 2 April 2021).
4. 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.

5. 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.
6. Kearney, A.T. Maintaining the Human Connection in an Age of AI 2019 Views from the C-Suite an Annual Survey of Global Business Executives. Available online: https://www.kearney.com/web/global-business-policy-council/views-from-the-c-suite (accessed on 2 April 2021).
7. AT&T. AT&T Cybersecurity Insights: The CEO's Guide to Securing the Internet of Things. Available online: https://www.business.att.com/content/dam/attbusiness/insights/migrated/exploringiotsecurity.pdf (accessed on 19 March 2021).
8. Congressional Research Service (CRS). The Internet of Things (IoT): An Overview. Available online: https://crsreports.congress.gov/product/pdf/IF/IF11239 (accessed on 2 April 2021).
9. Deloitte. Internet of Things (IoT) the Rise of the Connected World. Available online: https://www2.deloitte.com/in/en/pages/technology-media-and-telecommunications/articles/iot-2020.html (accessed on 2 April 2021).
10. IEC. IoT 2020: Smart and Secure IoT Platform. Available online: https://basecamp.iec.ch/download/iec-white-paper-iot-2020-smart-and-secure-iot-platform/ (accessed on 2 April 2021).
11. Juniper Research. IOT~THE INTERNET OF TRANSFORMATION 2020. Available online: https://www.juniperresearch.com/white-papers/iot-the-internet-of-transformation-2020 (accessed on 2 April 2021).
12. Lee, I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet* **2020**, *12*, 157. [CrossRef]
13. McKinsey & Company. How CEOs Can Tackle the Challenge of Cybersecurity in the Age of the Internet of Things. Available online: https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age (accessed on 2 April 2021).
14. McKinsey & Company. Growing Opportunities in the Internet of Things. Available online: https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things (accessed on 4 April 2021).
15. World Economic Forum. Future Series: Cybersecurity, Emerging Technology and Systemic Risk INSIGHT REPORT. Available online: http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf (accessed on 4 April 2021).
16. World Economic Forum. State of the Connected World 2020 Edition INSIGHT REPORT. Available online: http://www3.weforum.org/docs/WEF_The_State_of_the_Connected_World_2020.pdf (accessed on 2 April 2021).
17. McKinsey & Company. The 5G Era New Horizons for Advanced Electronics and Industrial Companies. Available online: https://www.mckinsey.com/industries/advanced-electronics/our-insights/the-5g-era-new-horizons-for-advanced-electronics-and-industrial-companies (accessed on 2 April 2021).
18. Garcia-Morchon, O.; Kumar, S.; Sethi, M. Internet of Things (IoT) Security: State of the Art and Challenges. *Internet Res. Task Force (IRTF)* **2019**, RFC8576. [CrossRef]
19. European Union. IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins). Available online: https://ec.europa.eu/jrc/en/publication/iot-20-and-internet-transformation-web-things-and-digital-twins (accessed on 2 April 2021).
20. HFS Research. HFS Top 10 Internet of Things (IoT) Service Providers 2019. Available online: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/generic/ey-hfs-top-ten-iot-service-providers-2019-excerpt-for-ey.pdf (accessed on 9 April 2021).
21. Bain & Company. Cybersecurity Is the Key to Unlocking Demand in the Internet of Things. Available online: https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things/ (accessed on 4 April 2021).
22. McKinsey & Company. Cybersecurity in a Digital Era Your Guide to the Emerging Technologies Revolutionising Business Now. Available online: https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-in-a-digital-era (accessed on 2 April 2021).
23. National Academy of Engineering. NAE GRAND CHALLENGES FOR ENGINEERING. Available online: http://www.engineeringchallenges.org/challenges/11574.aspx (accessed on 9 April 2021).
24. ECSO. State of the Art Syllabus v1 Overview of Existing Cybersecurity Standards and Certification Schemes. Available online: http://www.ecs-org.eu/documents/uploads/state-of-the-art-syllabus-v1.pdf (accessed on 20 July 2020).
25. Copper Horse. Mapping Security & Privacy in the Internet of Things. Available online: https://iotsecuritymapping.uk/ (accessed on 14 August 2020).
26. CSDE. The C2 Consensus on IoT Device Security Baseline Capabilities. Available online: https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf (accessed on 23 July 2020).
27. DCMS. Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/774438/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf (accessed on 14 August 2020).
28. ENISA. Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures. Available online: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (accessed on 20 July 2020).

29. NIST. IoT Device Cybersecurity Capability Core Baseline. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf (accessed on 7 January 2021).
30. ETSI. ETSI European Standard (EN) 303.645 Cyber Security for Consumer Internet of Things: Baseline Requirements. Available online: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (accessed on 21 July 2020).
31. W3C. Web of Things (WoT) Security and Privacy Guidelines. Available online: https://www.w3.org/TR/2019/NOTE-wot-security-20191106/#secure-practices-for-designing-a-thing-description (accessed on 23 July 2020).
32. Internet Engineering Task Force (IETF). CBOR Object Signing and Encryption (COSE). Available online: https://tools.ietf.org/pdf/rfc8152.pdf (accessed on 19 March 2021).
33. CTIA. CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.2.2. Available online: https://www.ctia.org/about-ctia/test-plans/ (accessed on 19 March 2021).
34. PSA JSA Members. PSA Certified™ Level 1 Questionnaire, Version 2.1. Available online: https://www.psacertified.org/getting-certified/device-manufacturer/level-1/ (accessed on 19 March 2021).
35. oneM2M. TR-0008-V2.0.1 Security (Technical Report). Available online: https://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf (accessed on 19 March 2021).
36. Moore, K.; Barnes, R.; Tschofenig, H. Best Current Practices for Securing Internet of Things (IoT) Devices. Available online: https://tools.ietf.org/html/draft-moore-iot-security-bcp-01 (accessed on 19 March 2021).
37. OWASP. OWASP Secure Coding Practices Quick Reference Guide. Available online: https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf (accessed on 19 March 2021).
38. Belk, M.; Coles, M.; Goldschmidt, C.; Howard, M.; Randolph, K.; Saario, M.; Sondhi, R.; Tarandach, I.; Vaha-Sipila, A.; Yonchev, Y. Fundamental Practices for Secure Software Development 2ND EDITION A Guide to the Most Effective Secure Development Practices in Use Today. Available online: http://safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf (accessed on 19 March 2021).
39. Ross, R.; McEvilley, M.; Carrier Oren, J. Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf (accessed on 19 March 2021).
40. AgeLight LLC. IoT Safety Architecture & Risk Toolkit, Version 4.0. Available online: https://www.agelight.com/iot (accessed on 23 February 2021).
41. AIOTI. Report on Workshop on Security and Privacy in the Hyper-Connected World. Available online: https://aioti.eu/aioti-wg03-reports-on-iot-standards/ (accessed on 22 July 2020).
42. Commonwealth of Australia. Code of Practice Securing the Internet of Things for Consumers. Available online: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf (accessed on 7 January 2021).
43. BITAG. Internet of Things (IoT) Security and Privacy Recommendations. Available online: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf (accessed on 22 July 2020).
44. CSA. Security Guidance for Early Adopters of the Internet of Things (IoT). Available online: https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf (accessed on 5 January 2021).
45. CSA. Identity and Access Management for the Internet of Things—Summary Guidance. Available online: https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf (accessed on 5 January 2021).
46. CSA. CSA IoT Security Controls Framework. Available online: https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/ (accessed on 6 May 2020).
47. GSM Association. GSMA IoT Security Assessment Checklist Version 3.0. Available online: https://www.gsma.com/iot/iot-security-assessment/ (accessed on 13 July 2020).
48. IIC. Industrial Internet of Things Volume G4: Security Framework. Available online: https://www.iiconsortium.org/IISF.htm (accessed on 6 January 2021).
49. IEEE. Internet of Things (IoT) Security Best Practices. Available online: https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_may_2017.pdf (accessed on 6 January 2021).
50. IoTSF. IoT Security Compliance Framework Release 2.1. Available online: https://www.iotsecurityfoundation.org/best-practice-guidelines/ (accessed on 20 July 2020).
51. IoTAC. IoT Security Guidelines Ver. 1.0. Available online: http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf (accessed on 13 August 2020).
52. NEMA. Cyber Hygiene Best Practices. Available online: https://www.nema.org/standards/view/cyber-hygiene-best-practices (accessed on 7 January 2021).
53. NIST. Foundational Cybersecurity Activities for IoT Device Manufacturers. Available online: https://doi.org/10.6028/NIST.IR.8259 (accessed on 7 January 2021).
54. OTA. IoT Security & Privacy Trust Framework v2.5. Available online: https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/ (accessed on 22 July 2020).
55. ENISA. Good Practices for Security of Internet of Things in the Context of Smart Manufacturing. Available online: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot (accessed on 20 July 2020).

56. ENISA. Good Practices for Security of IoT Secure Software Development Lifecycle. Available online: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1 (accessed on 5 January 2021).
57. ENISA. Procurement Guidelines for Cybersecurity in Hospitals Good Practices for the Security of Healthcare Services. Available online: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services (accessed on 5 January 2021).
58. ENISA. Guidelines for Securing the Internet of Things Secure Supply Chain for IoT. Available online: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things (accessed on 11 January 2021).
59. DHS. Strategic Principles for Securing the Internet of Things (IoT) Version 1.0. Available online: https://www.dhs.gov/securingtheIoT (accessed on 20 July 2020).
60. NHTSA. Cybersecurity Best Practices for Modern Vehicles. Available online: https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf (accessed on 8 January 2021).
61. DCMS. Code of Practice for Consumer IoT Security. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf (accessed on 14 August 2020).
62. UNESCO. Code of practice for scientific diving: Principles for the safe practice of scientific diving in different environments. In *UNESCO Technical Papers in Marine Science 53*; Flemming, N.C., Max, M.D., Eds.; United Nations Educational, Scientific and Cultural Organization: Paris, France, 1988.
63. ENISA. Task Forces on Terminology Definitions and Categorisation of Assets (TF-TDCA). Available online: https://www.enisa.europa.eu/publications/tf-tdca (accessed on 23 February 2021).
64. ISACA. ISACA Glossary. Available online: https://www.isaca.org/resources/glossary#glossg (accessed on 23 February 2021).
65. CSA. Guide to the CSA Internet of Things (IoT) Security Controls Framework. Available online: https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework/ (accessed on 6 May 2020).
66. NIST. Federal Information Processing Standards Publication (FIPS PUB) 199: Standards for Security Categorization of Federal Information and Information Systems. Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf (accessed on 6 May 2020).
67. NIST. Federal Information Processing Standards Publication (FIPS PUB) 200: Minimum Security Requirements for Federal Information and Information Systems. Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf (accessed on 6 May 2020).
68. Brass, I.; Pothong, K.; Haitham, M. Navigating and Informing the IoT Standards Landscape: A Guide for SMEs and Start-Ups. Available online: https://www.bsigroup.com/en-GB/navigating-and-informing-the-iot-standards-landscape/ (accessed on 21 July 2020).
69. IoTSF. IoT Security Compliance Questionnaire Release 2.1. Available online: https://www.iotsecurityfoundation.org/best-practice-guidelines/ (accessed on 20 July 2020).
70. 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 May 2020).
71. Maier, J.F.; Eckert, C.M.; John Clarkson, P. Model Granularity in Engineering Design—Concepts and Framework. *Des. Sci.* **2017**, *3*, e1. [CrossRef]
72. NIST. NIST Special Publication 800-37 Revision 2 Risk Management Framework for Information Systems and Organizations. Available online: https://doi.org/10.6028/NIST.SP.800-37r2 (accessed on 6 May 2020).
73. NIST. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf (accessed on 24 July 2020).
74. Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A Security Framework for the Internet of Things in the Future Internet Architecture. *Future Internet* **2017**, *9*, 27. [CrossRef]
75. R, J.; Chandran, P. Secure and Dynamic Memory Management Architecture for Virtualization Technologies in IoT Devices. *Future Internet* **2018**, *10*, 119. [CrossRef]
76. CSA Singapore and MEAC of the Netherlands. The IoT Security Landscape—Adoption and Harmonization of Security Solutions for the Internet of Things. Available online: https://www.csa.gov.sg/news/publications/iot-security-landscape (accessed on 6 May 2020).
77. AgeLight LLC. IoT Safety & Trust Design Architecture and Risk Assessment Toolkit. Available online: https://www.agelight.com/iot (accessed on 23 February 2021).