Contributions to Cybersecurity Risk Management: IoT Security Risk Management Strategy Reference Model (IoTSRM2)

A Thesis Submitted for obtaining
the Scientific Title of PhD in Engineering
from
Politehnica University Timișoara
in the Field of ENGINEERING AND MANAGEMENT
by

Eng. Traian Mihai POPESCU

PhD Committee Chair:
PhD Supervisor: Prof., Ph.D., eng. Gabriela Proștean
Scientific Reviewers:

Date of the PhD Thesis Defense: XX December 2021

The PhD thesis series of UPT are:

1.Automation
2.Chemistry
3.Energetics
4.Chemical Engineering
5.Civil Engineering
6.Electrical Engineering
7.Electronic Engineering and Telecommunications
8.Industrial Engineering
9.Mechanical Engineering
10.Computer Science and
Information Technology
11.Science and Material Engineering
12.Systems Engineering
13.Energy Engineering
14.Computers and Information Technology
15.Materials Engineering
16.Engineering and Management
17.Architecture
18.Civil Engineering and Installations
19.Electronics, Telecommunications
and Information Technologies

Politehnica University Timișoara, Romania, initiated the above series to disseminate the expertise, knowledge and results of the research carried out within the doctoral school of the university. According to the Decision of the Executive Office of the University Senate No. 14/14.07.2006, the series includes the doctoral theses defended in the university since October 1, 2006.

Romania, 300223 Timișoara, Bd. Vasile Pârvan no. 2B
Tel./fax +40-(0)256 404677
e-mail: editura@upt.ro

Foreword

This doctoral thesis is the result of my research activity in the Department of Management of the Politehnica University Timișoara (Romania).

Furthermore, this research activity has been supported by over a decade of cybersecurity and risk management experience including a master’s degree awarded with distinction from the Glasgow Caledonian University (UK), an international diploma in risk management awarded with distinction from the Institute of Risk Management (UK), hands-on security operations experience acquired as part of the global award winning Global Security Operations Centre of Zurich Insurance Company, and world-class cybersecurity consulting experience gained with Deloitte, PwC, and EY while based in Ireland, United Arab Emirates, and Spain, respectively.

First and foremost, I would like to thank my supervisor Prof., Ph.D., eng. Gabriela Proștean for providing me with the opportunity to undertake my PhD research study. Moreover, her ever insightful suggestions and great guidance allowed me to bring this research work to fruition. It was a tremendous privilege and very memorable experience for me to work with Prof., Ph.D., eng. Gabriela Proștean.

Finally, I would like to take this unique opportunity to share my gratitude to my wonderful wife Mădălina for her endless patience and support, my family, and friends.

Timișoara, December 2021 Traian Mihai Popescu

To my family

POPESCU, Traian Mihai

Contributions to Cybersecurity Risk Management: IoT Security Risk Management Strategy Reference Model (IoTSRM2)

PhD theses of UPT, Series X, No. YY, Editura Politehnica, 2021, 273 pages, 51 figures, 54 tables.

ISSN:
ISBN:
Keywords: Cybersecurity, risk management, Internet of Things, IoT security, cyber threat landscape, regulatory landscape, data protection and privacy, critical infrastructure protection, frameworks, best practices, threat rating, critical evaluation, reference model, information security strategy, survey design, benchmarking, NIST CSF.

Abstract:

This doctoral thesis provides contributions to the field of cybersecurity risk management, in particular to cybersecurity risk management drivers, cybersecurity risk management frameworks, and IoT security best practices. The main thesis contributions include:

- The critical evaluation of thirteen current cyber threat categories using a proposed threat rating method;
- The critical evaluation of cybersecurity-related legislations via a proposed evaluation method;
- The critical evaluation of cybersecurity risk management frameworks through a proposed evaluation methodology;
- The development of the IoT security risk management reference model (IoTSRM2) based on a proposed methodology, and the critical evaluations for the IoTSRM2;
- The undertaking of the IoTSRM2-based survey using a proposed survey methodology, the reporting of the survey findings, and the discussion on the IoTSRM2-based survey study.

TABLE OF CONTENTS

ACRONYMS

“3LoD”	“Three Lines of Defense”
“AI”	“Artificial Intelligence”
“AICPA”	“The American Institute of Certified Public Accountants”
“AIOTI”	“Alliance for Internet of Things Innovation”
“BEC”	“Business Email Compromise”
“BGP”	“Border Gateway Protocol”
“BITAG”	“Broadband Internet Technical Advisory Group”
“BSI”	“British Standards Institution”
“C2”	“Convening the Conveners”
“CA”	“Cybersecurity Act”
“CBOMs”	“Cybersecurity Bills of Materials”
“CBOR”	“Concise Binary Object Representation”
“CCM”	“Cloud Control Matrix”
“CFAA”	“Computer Fraud and Abuse Act”
“CIA”	“Confidentiality, Integrity, and Availability”
“CII”	“Critical Information Infrastructure”
“CIIP”	“Critical Information Infrastructure Protection”
“CIS”	“Center for Internet Security”
“CISOs”	“Chief Information Security Officers”
“CLOUD Act”	“Clarifying Lawful Overseas Use of Data Act”
“CMCA”	“Computer Misuse and Cybersecurity Act”
“CMDB”	“Configuration Management Database”
“COBIT”	“Control Objectives for Information and Related Technology”
“COSE”	“CBOR Object Signing and Encryption”
“COSO”	“Committee of Sponsoring Organizations of the Treadway Commission”
“CPS”	“Cyber-Physical Systems”
“CRR”	“Cyber Resilience Review”
“CSA”	“Cloud Security Alliance”
“CSA CCM”	“CSA Cloud Controls Matrix”
“CSDE”	“Council to Secure the Digital Economy”
“CSF”	“Cybersecurity Framework”
“CTOs”	“Chief Technology Officers”
“CX”	“Customer Experience”
“DDoS”	“Distributed Denial of Service”
“DFS”	“Department of Financial Services”
“DHS”	“Department of Homeland Security”
“DLT”	“Distributed Ledger Technology”
“DoS”	“Denial of Service”
“DSPs”	“Digital Service Providers”
“DX”	“Digital Transformation”
“EAR”	“Export Administration Regulations”
“EC”	“European Council”
“ECA”	“Export Controls Act”
“ECPA”	“Electronic Communications Privacy Act”
“EEA”	“European Economic Area”
“EMEA”	“Europe, Middle East and Africa”
“EN”	“European Standard”
“ENISA”	“The European Union Agency for Cybersecurity”

“ERM”	“Enterprise Risk Management”
“ETSI”	“European Telecommunications Standards Institute”
“ETT”	“ENISA Threat Taxonomy”
“EU”	“European Union”
“FAIR”	“Factor Analysis of Information Risk”
“FIPS”	“Federal Information Processing Standards”
“FIPS PUB”	“Federal Information Processing Standards Publication”
“GCI”	“Global Cybersecurity Index”
“GDPR”	“General Data Protection Regulation”
“GLBA”	“Gramm-Leach-Bliley Act”
“GSMA”	“GSM Association”
“HIPPA”	“Health Insurance Portability and Accountability Act”
“HTRA”	“Harmonized Threat and Risk Assessment”
“IAM”	“Identity and Access Management”
“IASME”	“The Standard of Information Assurance for Small and Medium sized Enterprises”
“ICMP”	“Internet Control Message Protocol”
“ICS”	“Industrial Control Systems”
“IDPS”	“Intrusion Detection and Prevention Systems”
“IEC”	“International Electrotechnical Commission”
“IEEE”	“Institute of Electrical and Electronics Engineers”
“IETF	“Internet Engineering Task Force”
“IIC”	“Industrial Internet Consortium”
“IIoT”	“Industrial Internet of Things”
“IoT”	“Internet of Things”
“IoTAC”	“IoT Acceleration Consortium”
“IoTSF”	“IoT Security Foundation”
“IoTSRM2”	“IoT Security Risk Management Strategy Reference Model”
“IP”	“Intellectual Property”
“IPA”	“Intelligent Process Automation”
“IRAM 2”	“The Information Risk Assessment Methodology 2”
“IRM”	“Institute of Risk Management”
“ISACA”	“Information Systems Audit and Control Association”
“ISF”	“Information Security Forum”
“ISMS”	“Information Security Management System”
“ISO”	“International Organization for Standardization”
“IT”	“Information Technology”
“IT-CMF”	“IT Capability Maturity Framework”
“ITGI”	“IT Governance Institute”
“ITIL”	“Information Technology Infrastructure Library”
“ITSM”	“Information Technology Service Management”
“ITU”	“International Telecommunication Union”
“ITU-T”	“ITU Telecommunication Standardization Sector”
“JSA”	“Joint Stakeholder Agreement”
“MADM”	“Multiple Attribute Decision Making”
“MIL”	“Maturity Indicator Level”
“MITRE CREF”	“MITRE’s Cyber Resiliency Engineering Framework”
“NEMA”	“National Electrical Manufacturers Association”
“NHTSA”	“US Department of Transportation National Highway Traffic Safety Administration”
“NISD”	“Directive on Security of Network and Information Systems”
“NIST”	“National Institute of Standards and Technology”
“NIST CSF”	“NIST’s Framework for Improving Critical Infrastructure Cybersecurity”
“NIST UISF”	“NIST’s Unified Information Security Framework”
“NY”	“New York”
“NYFSC”	“New York’s Department of Financial Services Cybersecurity Regulation”

“OCTAVE”	“The Operationally Critical Threat, Asset, and Vulnerability Evaluation”
“OEMs”	“Original Equipment Manufacturers”
“OES”	“Operators of Essential Services”
“OT”	“Operational Technology”
“OTA”	“Online Trust Alliance”
“OTT”	“Open Threat Taxonomies”
“OWASP”	“The Open Web Application Security Project”
“PAS”	“Publicly Available Specification”
“PCI/DSS”	“Payment Card Industry Data Security Standard”
“PDPA”	“Personal Data Protection Act”
“PII”	“Personally Identifiable Information”
“PSA”	“Platform Security Architecture”
“PSD2”	“Payment Services Directive 2”
“RAM”	“Risk Assessment Method”
“RATs”	“Remote Access Trojans”
“RMF”	“Risk Management Framework”
“RPA”	“Robotic Process Automation”
“RQ”	“Research Question”
“SABSA”	“Sherwood Applied Business Security Architecture”
“SAFECode”	“Software Assurance Forum for Excellence in Code”
“SDLC”	“Software Development Lifecycle”
“SEI”	“Software Engineering Institute”
“SLOs”	“Service Level Objectives”
“SME”	“Small and Medium Sized Enterprise”
“SPs”	“Special Publications”
“STRIDE”	“spoofing identity, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege”
“SYN”	“Synchronize”
“TCP”	“Transfer Control Protocol‟
“TOCSR”	“Taxonomy of Operational Cyber Security Risks”
“TPPs”	“Third Party Payment Service Providers”
“TTPs”	“Tactics, Techniques, and Procedures”
“UDP”	“User Datagram Protocol”
“UIDs”	“Unique Identifiers”
“UK”	“United Kingdom”
“UK DCMS”	“United Kingdom Department for Digital, Culture, Media and Sport”
“US”	“United States”
“TMT”	“Technology, Media, & Telecom”
“TWG”	“Technical Working Group”

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Nowadays, organizations from all over the world leverage technological advances at an unprecedented pace while operating in a risky business environment that is shaped by the proliferation of rampant cyber threats and the ever-changing cybersecurity regulatory landscape. From a cybersecurity perspective this status quo is quite worrying for many organizations as they rely on reactive cybersecurity-related strategies, and it is more worrying when they embrace IoT technologies.

Given the prevalence of poor cybersecurity risk management practices and the widespread absence of robust IoT security risk management strategies in organizations, the purpose of this doctoral thesis is to contribute to the improvement of the cybersecurity risk management and of the IoT security risk management strategy in particular. In this context, this thesis aims to support cybersecurity practitioners to frame or reframe their cybersecurity-related risk management strategies in advance of future cyber attacks.

Thus, considering that strategic analysis is of paramount importance to strategy formulation and that leveraging planning instruments is essential for developing actionable strategies, first, this thesis focuses on providing overviews of the key drivers of and enablers for cybersecurity risk management. With respect to the key drivers, the thesis provides an overview of the cyber threat landscape by consolidating thirteen current cyber threat categories and an overview of the key cybersecurity-related legislations and regulations in three selected jurisdictions. With respect to the key enablers, the thesis provides an overview of several well-renowned cybersecurity risk management frameworks and an overview of some of the key IoT security best practices using a proposed taxonomic hierarchy.

Then, the thesis extends the research on the cybersecurity risk management drivers by critically evaluating the thirteen cyber threat categories based on the proposed cyber threat rating method and critically evaluating the in-scope cybersecurity-related legislations and regulations based on the proposed method for evaluating cybersecurity-related legislations from the perspective of organizational understanding to managing cybersecurity risk.

Afterwards, the thesis extends the research on the cybersecurity risk management frameworks by critically evaluating eight cybersecurity risk management frameworks based on the proposed methodology for evaluating cybersecurity risk management frameworks.

Furthermore, the thesis extends the research on IoT security best practices by proposing a methodology for developing the IoT security risk management strategy reference model (IoTSRM2) based on cybersecurity risk management and IoT security best practices, developing the IoTSRM2 based on the proposed methodology, critically evaluating seven informative references in relation to the proposed IoTSRM2, and providing the related work for the proposed IoTSRM2. Then, this research work is further extended by proposing a survey methodology based on the IoTSRM2 and survey design best practices to address 14 research questions, undertaking the IoTSRM2-based survey, analysing the survey responses, reporting the survey findings, and providing the related work for the IoTSRM2-based survey study.

1. INTRODUCTION

1.1. Background of the Doctoral Thesis

This subchapter provides the background of cybersecurity risk management and then it provides the background of Internet of Things (IoT).

1.1.1. Cybersecurity Risk Management: Background

Based on the information disseminated by the author through the research paper [Giu+21], cyberspace is "a man-made digital ecosystem interconnecting organizations, people, processes, and technologies online, including the Internet, telecommunications networks, business processes, technology components, and resident information being in use, in motion or at rest [Cab11a], [Uni14], [Ban16], [ETS17]" [Giu+21]. It enables "system interconnections, streamlined operations, market reach, instant communications, and massive information exploitation and dissemination across remote locations [Ban16]" [Giu+21].

Based on the information disseminated by the author through the research paper [Giu+21], nowadays, organizations are innovating at an unprecedented pace and investing in "Digital Transformation (DX)" initiatives worldwide by "increasingly leveraging cyberspace and emerging digital technologies including cloud computing [Lon+12], [Lon+13a], Distributed Ledger Technology (DLT), Internet of Things (IoT)/connected devices and sensors, Robotic and Intelligent Process Automation (RPA and IPA), Artificial Intelligence (AI), advanced data analytics, mobile and social technologies, and novel digital solutions, to drive intelligence-led decision-making, bring new operational efficiencies, enhance Customer Experience (CX), accelerate productivity, and achieve commercial or governmental edge, significant economic benefits, and growth [Pop+18], [EY18a], [ENI18a], [EY17a], [WEF18a], [PwC17]" [Giu+21]. Notwithstanding, institutional digitalization and interconnection in the cyberspace "are expanding the attack surface of modern organizations through infusion of complexity and diversification of attack avenues to Information Technology (IT) and Operational Technology (OT) infrastructures, while generating enormous amounts of data including operational and financial information, Intellectual Property (IP), trade secrets, or Personally Identifiable Information (PII) that can be harnessed by hostile actors ranging from organized crime to state-sponsored agents trying to abuse this data [Pop+18], [ENI18a], [PwC18], [Ali+14], [Lin+18], [ISF14], [PwC16], [Del12]" [Giu+21].

Furthermore, based on the information disseminated by the author through the research paper [Giu+21], the global cyber threat landscape is "incessantly evolving and sophisticating predominantly driven by monetization of cybercrime and espionage motives of rampant cyber offenders competing or joining forces to outmaneuver cyber defenders and gain greater rewards from the ubiquitous DX race [EY18a], [ENI18a], [Ali+14], [Lin+18], [Ver18], [Del17a], [EY14]" [Giu+21]. These omnipresent threat agents are accelerating innovation in cybercrime space by "sharing cyber threat intelligence and capitalizing on the anonymity of darknets and cryptocurrency along with the escalating cyber dependency, and consequently, are advancing their tradecraft and Tactics, Techniques, and Procedures (TTPs) to effectively orchestrate upscaled cyberattacks and achieve their intended malicious outcomes [ENI18a], [Ali+14], [WEF18b], [Eur17], [IBM18a], [Mav+17]" [Giu+21]. Hence, recent threat related research in the cyberspace highlighted "the worrying proliferation of threat agents and attack vectors, and revealed malware including self-propagating ransomware (e.g., WannaCry and NotPetya outbreaks), information stealing banking Trojans botnets (e.g., Dridex, Ramnit, Emotet), Remote Access Trojans (RATs) (e.g., Gh0st), mobile malware, and other malicious software, as one of the most prominent cyber threats with respect to the mass and diversity of the potential targets and the probable magnitude of impact [ENI18a], [Ver18], [Eur17], [IBM18a], [CIS18a], [BSI17]" [Giu+21].

Consequently, based on the information disseminated by the author through the research paper [Giu+21], "the risks of confidential information exfiltration and industrial espionage, data leakage, critical infrastructure sabotage, information system tampering, prolonged service disruption, and the like, which in turn might result in adverse consequences such as penalties or legal liabilities, financial distress, reputational harm, brand depreciation, or worse, in the cyberspace are relentlessly intensifying both in prevalence and disruptive potential [ISF14], [WEF18b], [Deu+14]" [Giu+21]. Furthermore, according to the research study conducted by Juniper Research in 2017, "the costs associated with cyber-attacks are estimated to amount to over USD 8 trillion in the next five years [WEF18b], [Eur17], [Jun17]" [Giu+21]. In this context, based on the information disseminated by the author through the research paper [Giu+21], "the holistic process of protecting the Confidentiality, Integrity, and Availability (CIA triad) of information and information systems and controlling access to information in the cyberspace by identifying, assessing, and responding to cybersecurity and privacy risks at all levels is paramount to successfully prevent, detect, and respond to cyber attacks or other adverse events linked to cyber harm through people, processes and technology, and to effectively de-risk the cybersecurity posture of organizations [Pop+18], [PwC18], [Deu+14], [NIS18a], [ENI17a]" [Giu+21]. In other words, cybersecurity risk management becomes of particular importance to effectively address cybersecurity and privacy risks [Giu+21].

Furthermore, based on the information disseminated by the author through the research paper [Giu+21], authority structures including country governments and authorities from multiple jurisdictions "have reacted to address these issues resulting from the ongoing digital revolution and the ever-escalating cyber threat landscape by sanctioning more demanding statutory and regulatory requirements to regulate the conduct pertaining to governing and managing cyber and data privacy risks, and to prescribe organizations to prove compliance with applicable cybersecurity mandates [EY17a], [Ali+14], [Del17a], [BSI17], [May18]" [Giu+21]. Thus, based on the information disseminated by the author through the research paper [Giu+21], a few notable examples of regulatory initiatives include:

- "General Data Protection Regulation (GDPR) imposing heavy sanctions worldwide on organizations for non-compliance with the protection of privacy and PII of European Union (EU) citizens [BSI17], [Del18a]" [Giu+21];
- "Payment Services Directive 2 (PSD2) mandating banks to open their IT infrastructure to Third Party Payment Service Providers (TPPs) for better payment efficiency while having to ensure greater payments security and fraud protection [BSI17], [EY17b]" [Giu+21];

- “Directive on Security of Network and Information Systems (NIS Directive) requiring EU member states to transpose the NIS Directive in their national laws by May 2018, and within six more months, to identify the Operators of Essential Services (OES) and Digital Service Providers (DSPs) (i.e., operators of critical infrastructures) which will be subject to the NIS Directive including risk management and incident reporting obligations [BSI17], [EY17c], [ENI16a]” [Giu+21];
- “New York State (NY) Department of Financial Services (DFS) cybersecurity requirements mandating NY DFS-regulated organizations to meet specific cybersecurity requirements including, among others, to design, implement, and maintain a cybersecurity programme, and undergo annual certification for compliance with the NY DFS [EY17d], [Del18b]” [Giu+21].

In this context, based on the information disseminated by the author through the research paper [Giu+21], organizations are faced with “a clear need for improving the maturity of their cybersecurity risk management capabilities to keep pace with the ever-evolving cyber threats, accelerated institutional digitalization, and more and more stringent domestic and cross-border security and privacy legal and regulatory requirements” [Giu+21]. Meanwhile, national and international standardization bodies along with multiple other entities “strive in supporting and steering organizations to enhance their cybersecurity maturity stance and achieve greater compliance through various cybersecurity risk management works involving the development of frameworks, standards, voluntary guidance, and best practices that can be leveraged by organizations to fuel their cybersecurity risk management initiatives [May18]” [Giu+21]. In a very simplified form, the strategic outcomes of these initiatives can be divided into two categories: frameworks and framework enablers (e.g., standards, methodologies). In this view, these initiatives are centered around cybersecurity risk management frameworks and that is why a subchapter (i.e., Chapter 2.3) is dedicated to providing an overview of these frameworks and a separate chapter (i.e., Chapter 4) is dedicated to discussing some of these frameworks.

Thus, the remaining of this sub-subchapter focuses on defining and outlining cybersecurity risk management concepts. Then the subchapter focuses on defining and providing a few examples with description of some of the most widespread standards, methodologies, and methods as “these terms are used inconsistently in the literature surrounding the cybersecurity risk management topic and because exploring all possible framework enablers would be impracticable within the scope of this subchapter” [Giu+21]. The overview of cybersecurity risk management standards, methods, and methodologies was also discussed in one of my research papers [Giu+21] and in my first PhD report [Pop20].

1.1.1.1 Cybersecurity Risk Management Concepts

This sub-sub-subchapter provides the definitions of selected terms, presents the cybersecrurity risk management process, and outlines the key domains relevant for a cybersecurity risk management strategy.

First, this sub-sub-subchapter defines selected terms that are relevant for cybersecurity risk management:

- **“Cybersecurity”:** the process of protecting the Confidentiality, Integrity, and Availability (CIA triad) of information and information systems and controlling access to information in the cyberspace by preventing, detecting, and responding to cyber attacks [NIS18a];
- **“Confidentiality”:** the property that information is preserved secret to unauthorized entities [NIS19a];
- **“Integrity”:** the property that data has not been tampered by unauthorized entities or altered in an accidental way [NIS19a];
- **“Availability”:** the property that assets are readily accessible to and usable by authorized entities in a reliable manner [NIS19a];
- **“Cybersecurity strategy”:** the strategy that makes way for a cybersecurity programme, addresses how organizations intend to go about preventing, detecting, and responding to cyber attacks, and aims to achieve cyber resilience and other intended outcomes [Sto21], [NIS19a];
- **“Cybersecurity programme”:** a programme established, implemented, and maintained to assure adequate cybersecurity [NIS19a];
- **“Cyber resilience”:** the ability to adapt to dynamic conditions, maintain essential operational capabilities at all times, and withstand and recover in time from adverse cyber events [CNS15], [NIS11], [NIS19a];
- **“Vulnerability”:** weakness in an information system or system security or privacy controls (i.e., administrative, technical, and physical) that may be exploited or triggered by a cyber threat [NIS12a], [NIS19a];
- **“Attack surface”:** the set of points on the boundary of a system, a system element, or an environment where an attacker could exploit a vulnerability [NIS19a];
- **“Cyber threat”:** any event that may harm organizational operations, assets, or stakeholders through an information system by exercising (i.e., triggering or exploiting) a vulnerability [NIS19a];
- **“Cyber attack”:** an attack, via cyberspace, that harms organizational operations, assets, or stakeholders for the purposes of achieving malicious outcomes [ENI17a], [NIS19a];
- **“Cybercrime”:** any criminal activity facilitated through cyberspace [ENI17a];
- **“Cyber harm”:** any adverse impact on an individual or organization (i.e., physical or digital, economic, psychological, reputational, social or societal) that would be caused if a cyber threat exercises a vulnerability [NIS19a];
- **“Cybersecurity risk”:** a measure of the extent to which an organization is threatened by a cyber threat, and typically a function of the corresponding degree of cyber harm and likelihood of this harm occurring [NIS12a], [NIS19a];
- **“Privacy risk”:** a measure of the extent to which an organization is threatened by the loss of control over personal information, and typically a function of the corresponding degree of harm and likelihood of this harm occurring [NIS19a];
- **“Cybersecurity risk management”:** coordinated activities to direct and control the approach to identifying, assessing, responding to, and monitoring cybersecurity risk [ISO18c] [NIS18a];
- **“Cybersecurity risk management strategy”:** the strategy that addresses how organizations intend to identify, assess, respond to, and monitor cybersecurity risk, while making explicit the cybersecurity risk appetite and tolerance statements [NIS19a];
- **“Cybersecurity risk appetite”:** broad-based amount of cybersecurity risk, an organization is willing to accept in pursuit of its mission objectives [NIS19a];

- **"Cybersecurity risk tolerance":** the level of cybersecurity risk that is acceptable to organizations [CNS15], [NIS19a].

Then, Fig. 1.1 presents a general overview of a cybersecurity risk management process. This cybersecurity risk management process involves certain activities that can be cyclical (i.e., depending on the degree of sufficiency of information derived from the risk assessment and/or risk treatment activities) for refinement purposes, and it is comprised of context establishment, cybersecurity risk assessment (i.e., "risk identification", "risk analysis", and "risk evaluation"), cybersecurity risk treatment, cybersecurity risk acceptance, cybersecurity risk communication and consultation, and cybersecurity risk monitoring and review [ISO18c]. First, the context establishment or risk framing according to the NIST, establishes the context in which risk-based decisions are made [NIS11]. Moreover, this framing of cybersecurity risk produces a cybersecurity risk management strategy as its principal output, which defines, inter alia, the scope, assumptions (i.e., to enable consistent characterization/determination of cyber threats, vulnerabilities, cyber harm, and likelihood of cyber harm occurrence), constraints (e.g., financial limitations, regulatory requirements, cultural constraints), cybersecurity risk tolerance (e.g., levels of risk, types of risk), priorities, and approach for managing cybersecurity risk [NIS11], [NIS12a]. Second, the cybersecurity risk assessment identifies, analyzes (i.e., using qualitative and/or quantitative risk analysis methods), and evaluates the cybersecurity risk [ISO18c]. This assessment of cybersecurity risk involves the identification of cyber threats, the discovery of vulnerabilities, and the determination of cybersecurity risk (i.e., by looking at cyber threats, vulnerabilities, likelihoods, and cyber harms) [NIS11], [NIS12a].

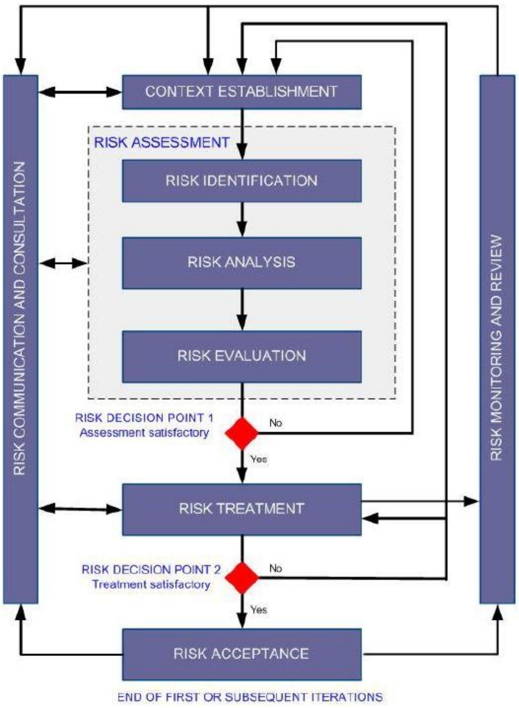


Fig. 1.1. A cybersecurity risk management process [ISO18c]

Third, the cybersecurity risk treatment and risk acceptance make up the cybersecurity risk response component that involves the identification of cybersecurity risk response (i.e., accept/retain, avoid, mitigate/reduce, or share/transfer the risks), the evaluation of alternative courses of action for cybersecurity risk response, the decision on the appropriate course of action for cybersecurity risk response (i.e., based on the risk tolerance), and the implementation of the selected course of action for cybersecurity risk response [NIS11]. Then, the cybersecurity risk monitoring and review or risk monitoring according to the NIST, identifies cybersecurity risk-impacting changes to the organizational context (i.e., to information systems and environments of operation) and monitors and reviews the cybersecurity risk management process for continuous improvement [ISO18c]. In addition, the cybersecurity risk monitoring involves the development of a cybersecurity risk monitoring strategy that guides the compliance monitoring (i.e., to ensure that the needed implementation of cybersecurity risk response is achieved), the effectiveness monitoring (i.e., to ensure that the implemented cybersecurity risk response is effective), the monitoring of changes (i.e., to ensure that the awareness of cybersecurity risk-impacting changes is maintained), the degree of automation employed for cybersecurity risk monitoring (i.e., to ensure that automation is employed where feasible instead of relying on manual monitoring), and the frequency of the monitoring activities [NIS11]. Finally, the cybersecurity risk communication and consultation which is associate with the entire cybersecurity risk management process involves the exchange of cybersecurity risk information between the key stakeholders [ISO18c].

Furthermore, given that the cybersecurity risk management strategy guides and underpins the cybersecurity risk management, this sub-sub-subchapter briefly outlines the key domains of the cybersecurity risk management strategy. Moreover, according to the NIST [NIS18b], the cybersecurity risk management strategy aligns with the "NIST Cybersecurity Framework (CSF) Identify Function" (i.e., establishes an organizational understanding for managing cybersecurity risk) [NIS18a]. Thus, the key domains of the cybersecurity risk management strategy correspond to the six categories of the "NIST CSF Identify Function" (i.e., groups of cybersecurity outcomes), namely:

- **"Asset Management (ID.AM)":** the organization's assets (e.g., data, personnel, devices, systems, and facilities) are identified and managed in line with their criticality to organization's mission objectives and enterprise risk management strategy [NIS18a];
- **"Business Environment (ID.BE)":** the organization's mission, objectives, stakeholders, activities, and priorities are understood, and they inform the cybersecurity roles, responsibilities, and risk management decisions [NIS18a];
- **"Governance (ID.GV)":** the administrative cybersecurity controls (e.g., policies, procedures, processes) to manage the organization's constraints (e.g., regulatory, legal, risk, environmental, and operational requirements) are established, understood, and inform the cybersecurity risk management [NIS18a];
- **"Risk Assessment (ID.RA)":** the organization's cybersecurity risk to organizational operations (including mission, functions, image, or reputation), assets, and stakeholders is identified, analysed, evaluated, and understood [NIS18a];
- **"Risk Management Strategy (ID.RM)":** the organization's priorities, constraints, risk tolerances, and assumptions for managing cybersecurity risk are

established, understood, and used to support the making of cybersecurity risk-based decisions [NIS18a];

- **"Supply Chain Risk Management (ID.SC)":** the organization's priorities, constraints, risk tolerances, assumptions, and processes for managing cybersecurity risk are established, understood, and used to support the making of risk-based decisions with regard to cyber supply chain risk management [NIS18a].

1.1.1.2 Cybersecurity Risk Management Standards

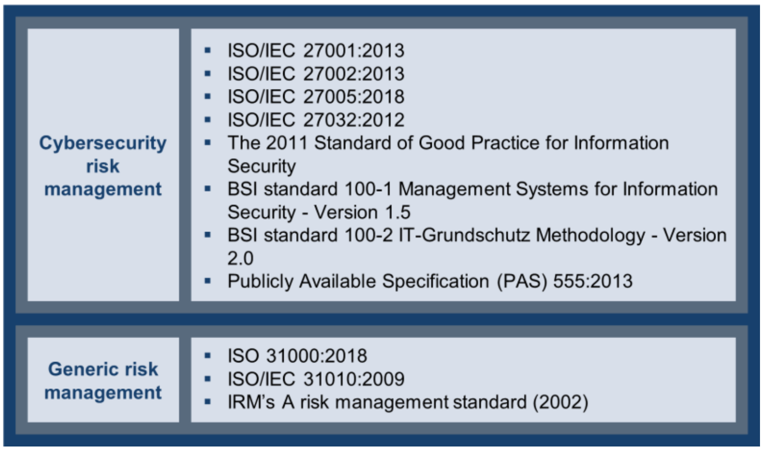
The definition of a "standard" provided in this sub-sub-subchapter "is derived from and based on the definitions of the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), International Telecommunication Union (ITU), and British Standards Institution (BSI)" [Giu+21]. Based on the information disseminated by the author through the research paper [Giu+21], the term "standard" is defined as "an agreed best practice developed by an external standards organization which consists of requirements, specifications, guidelines or characteristics for activities or for their results, that are generally complied with for making a product, managing a process, delivering a service or supplying materials". Furthermore, "standards cover a wide range of subjects and are widely adopted by organizations, used by their customers, and applied for reference in national and international laws or regulations [ISO18a], [IEC18], [ITU18], [BSI18]" [Giu+21].

From the myriad of standards relevant to cybersecurity risk management [ISO18b], [Cro13], [ENI15], this overview of the most common standards (see Table 1.1 and Table 1.2) focuses on "selecting various widely used cybersecurity and risk management standards which are not specifically targeting products or services and can be leveraged by any organization regardless of type, size, or sector" [Giu+21]. Therefore, based on the information disseminated by the author through the research paper [Giu+21], the categories of standards pertaining to cybersecurity risk management that are considered beyond the scope of this overview are enumerated below along with a couple of examples of standards corresponding to each category:

- "Standards related to individual products or services" [ISO18b], [Cro13], [ENI15], [CSC16], [ISA16], [Giu+21]:
  - "Federal Information Processing Standards Publication (FIPS) Publication 140-2 published by National Institute of Standards and Technology, provides security requirements for cryptographic modules"
  - "ISO/IEC 27039:2015 provides guidelines for assisting organizations in selecting, deploying, and operating Intrusion Detection and Prevention Systems (IDPS)"
  - "Standards specifically targeting cloud services (e.g., ISO/IEC 27017:2015, ISO/IEC 27018:2014)"
  - "ISO/IEC 17021 consists of requirements for bodies providing audit and certification of management systems"
  - "ISA/IEC 62443 series of standards on the cyber security of industrial automation and control systems"
- "Standards describing sector-related security guidelines" [ISO18b], [Cro13], [ENI15], [CSC16], [Giu+21]:

  - "Payment Card Industry Data Security Standard (PCI/DSS) version 3.2.1 for financial services issued by PCI Security Council"
  - "ISO/IEC 27011 for telecommunication industry"
  - "Health Insurance Portability and Accountability Act (HIPPA) for healthcare"
  - "ISO/IEC 27019 for energy utility industry"
- "Standards developed to be adhered by a specific type of organization", such as [Cro13], [Giu+21]:
  - "HMG Information Assurance Standard no. 6 (2011) issued by Cabinet Office and CESG for protecting personal data and managing information risk; it is aimed for central government departments, agencies, their suppliers and service providers [Cab11b]"
- "Standards developed to be adhered by a specific organization size", such as [Cro13], [Giu+21]:
  - "The Standard of Information Assurance for Small and Medium sized Enterprises (IASME)"

In short, this overview of standards is focused on two categories of standards: "cybersecurity risk management" and "generic risk management" [Giu+21]. Further, Fig. 1.2 outlines the selected standards relevant to each of the two categories of standards.



Cybersecurity risk management	▪ ISO/IEC 27001:2013 ▪ ISO/IEC 27002:2013 ▪ ISO/IEC 27005:2018 ▪ ISO/IEC 27032:2012 ▪ The 2011 Standard of Good Practice for Information Security ▪ BSI standard 100-1 Management Systems for Information Security - Version 1.5 ▪ BSI standard 100-2 IT-Grundschutz Methodology - Version 2.0 ▪ Publicly Available Specification (PAS) 555:2013
Generic risk management	▪ ISO 31000:2018 ▪ ISO/IEC 31010:2009 ▪ IRM's A risk management standard (2002)

Fig. 1.2. Selected standards related to cybersecurity risk management [Pop20]

Hence, based on the information disseminated by the author through the research paper [Giu+21], the tables below (i.e., Table 1.1 and Table 1.2) provide an overview of the selected standards relevant to cybersecurity risk management by mapping the standards to their corresponding category (i.e., "cybersecurity risk management", and "generic risk management"), and each table provides for each standard the following details: "publisher name", "short description", and "access (i.e., free of charge, not freely available, freely available to members)" [Giu+21]. As shown in Table 1.1, the selected "cybersecurity risk management standards" provide requirements for the "Information Security Management System (ISMS)", general guidelines for the "ISMS", general guidelines for information security risk management, guidelines for cybersecurity, or requirements for cybersecurity risk management.

Table 1.1. Overview of selected cybersecurity risk management standards [Giu+21]

Standard Name	Publisher	Description	Access
"ISO/IEC 27001:2013"	"ISO and IEC"	"Provides requirements for establishing, implementing, reviewing, maintaining, and improving an information security management system [ISO18b], [ENI06], [Cro13], [ISO13a]" [Giu+21].	Not freely available
"ISO/IEC 27002:2013"	"ISO and IEC"	"It is a code of practice for information security controls which provides general guidelines for the selection and implementation of security controls [ISO18b], [ISO13b]" [Giu+21].	Not freely available
"ISO/IEC 27005:2018"	"ISO and IEC"	"Provides general guidelines for information security risk management by describing the information security risk management process from context establishment to communication and consultation; it is the updated version of ISO/IEC 27005:2011 standard [ISO18b], [ISO18c], [ENI06], [Tau14]" [Giu+21].	Not freely available
"ISO/IEC 27032:2012"	"ISO and IEC"	"It is twofold: firstly, it specifies cybersecurity guidelines for improving the state of cybersecurity by introducing technical cybersecurity controls to protect against common cybersecurity risks in the cyberspace, and secondly, it provides a framework to enable stakeholders to share cybersecurity information and handle security incidents [Del12], [ISO18b], [WIS16], [ISO12]" [Giu+21].	Not freely available
"The 2011 Standard of Good Practice for Information Security"	"Information Security Forum (ISF)"	"Addresses four categories of information security good practice (i.e., security governance, security requirements, control framework, and security monitoring and improvement). For each category the standard provides a number of security-related areas under which it describes their corresponding topics with associated set of statements [ISF11]" [Giu+21].	Freely available to members
"BSI standard 100-1 Management Systems for Information Security (ISMS) - Version 1.5"	"Federal Office for Information Security of Germany (BSI Germany)"	"Provides general requirements for an Information Security Management System (ISMS) which are defined as part of the overview given for each of the four components of an ISMS (i.e., management principles, resources for IT operations and information security, involving personnel in the information security process, and information security process). This standard was designed to be fully compatible with ISO/IEC 27001 standard [BSI08a]" [Giu+21].	Free of charge

Standard Name	Publisher	Description	Access
"BSI standard 100-2 IT-Grundschutz Methodology - Version 2.0"	"Federal Office for Information Security of Germany (BSI Germany)"	"Provides a detailed description of the activities involved in implementing the requirements defined as part of the BSI Standard 100-1, that are to be used for setting up and operating an ISMS [BSI08b]" [Giu+21].	Free of charge
"Publicly Available Specification (PAS) 555:2013"	"British Standards Institution (BSI UK)"	Titled "Cyber security risk. Governance and management. Specification", it consists "of requirements for governing and managing cyber security risks and addresses the cyber security technical aspects, the physical, cultural and behavioral measures, together with effective leadership and governance [ENI15]" [Giu+21].	Not freely available

Based on the information disseminated by the author through the research paper [Giu+21], while Table 1.1 shows the overview of the selected standards relevant to "cybersecurity risk management" category issued by "ISO/IEC", "ISF", "BSI UK", and "BSI Germany", Table 1.2 provides an overview of selected standards relevant to "generic risk management" category published by "ISO", "IEC", and "the Institute of Risk Management (IRM)" [Giu+21]. As shown in Table 1.2, the selected "generic risk management standards" provide principles and guidelines on risk management or guidelines on risk assessment.

Table 1.2. Overview of selected generic risk management standards [Giu+21]

Standard Name	Publisher	Description	Access
"ISO 31000:2018"	"ISO"	"Provides principles on risk management and guidelines on risk management framework and process, and it is cross-industry and cross-sector [IRM18]; it is the revised version of ISO 31000:2009 [ISO18d]" [Giu+21].	Not freely available
"ISO/IEC 31010:2009"	"ISO and IEC"	"Provides an overview of risk assessment concepts and process having a separate section for describing the selection of risk assessment techniques by defining the relevant factors to be considered while making the selection (i.e., availability of resources, the nature and degree of uncertainty, and complexity) and describing a range of risk assessment techniques for selection and adoption while conducting risk assessments [ISO09], [Cro17]" [Giu+21].	Not freely available
"A risk management standard (2002)"	"The Institute of Risk Management"	"Provides a description of the risk management process with its associated activities including assessing (i.e., analyzing and evaluating), treating, reporting, and monitoring risks for the purpose of meeting the organization's strategic objectives throughout the entire risk management process [IRM02]" [Giu+21].	Free of charge

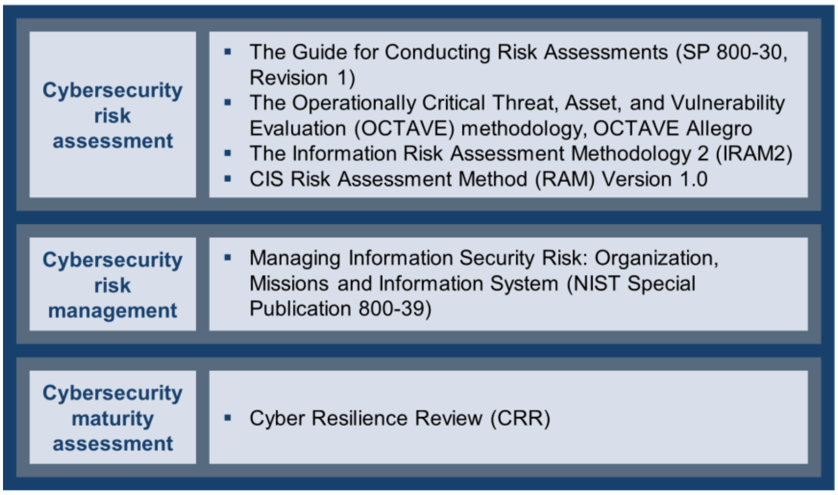
1.1.1.3 Cybersecurity Risk Management Methodologies

Considering that “the terms methodology and method are used either interchangeably or as having different meanings”, it is important to “avoid any confusion and delineate a clear distinction between the two terms at first [Mac+06]” [Giu+21]. Hence, based on the information disseminated by the author through the research paper [Giu+21], a method can be defined as “a focused mode of applying systematic rules, procedures or tools providing a logical path and sequence of actions for data collection and analysis to produce information and complete an activity or obtain a result [Ion13], [Mac+06], [Gha+10]” [Giu+21]. As for methodology, based on the information disseminated by the author through the research paper [Giu+21], this can be viewed as “the recommended series of orderly activities based on certain rational, designed to accomplish a specific objective or other intended outcome enabling the overall approach to a particular engagement or initiative [Pal+03], [Avi+02]” [Giu+21]. Consequently, based on the information disseminated by the author through the research paper [Giu+21], it can be argued that “risk assessment and management methodologies guide the structure of the risk assessment and management processes which are much broader than the many underlying methods that may support the multiple activities involved in these processes”. For illustration, “according to the National Institute of Standards and Technology (NIST) an assessment method is the action of examining, interviewing, or testing for evidence collection during an assessment, whereas a risk assessment methodology is a risk assessment process, together with an explicit risk model, a method type to assess risks (e.g., quantitative, qualitative, or semi-qualitative), and a preset focus [NIS13], [NIS12a]” [Giu+21].

As “there are quite a few risk assessment and management methodologies mentioned in the literature” [Giu+21], this sub-sub-subchapter concentrates on merely a few notable methodologies. In this sense, this sub-sub-subchapter provides a few methodologies unveiling characteristics that “resemble a particular category pertaining to cybersecurity risk management”, specifically [Giu+21]:

- “Cybersecurity risk assessment”;
- “Cybersecurity risk management”;
- “Cybersecurity maturity assessment”.

Further, Fig. 1.3 highlights the methodologies selected for each of the aforementioned categories.



Cybersecurity risk assessment	▪ The Guide for Conducting Risk Assessments (SP 800-30, Revision 1) ▪ The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology, OCTAVE Allegro ▪ The Information Risk Assessment Methodology 2 (IRAM2) ▪ CIS Risk Assessment Method (RAM) Version 1.0
Cybersecurity risk management	▪ Managing Information Security Risk: Organization, Missions and Information System (NIST Special Publication 800-39)
Cybersecurity maturity assessment	▪ Cyber Resilience Review (CRR)

Fig. 1.3. Selected cybersecurity risk management methodologies [Pop20]

Therefore, based on the information disseminated by the author through the research paper [Giu+21], Tables 1.3, 1.4, and 1.5 "highlight a few widely adopted methodologies corresponding to the aforementioned categories and useful for conducting cybersecurity risk assessments, managing cybersecurity risks, and establishing the organization's maturity state of cybersecurity practices by benchmarking the current state against peer organizations or a pre-defined target maturity state based on a capability maturity model (i.e., designed according to standards and best practice or regulatory requirements)" [Giu+21]. Moreover, these tables provide additional details mapped against each methodology including: "the publisher", "a short description", along with "the corresponding access (i.e., free of charge, not freely available, freely available to members)" [Giu+21].

Table 1.3. Overview of selected cybersecurity risk assessment methodologies [Giu+21]

Methodology Name	**Publisher**	**Description**	**Access**
"The Guide for Conducting Risk Assessments (SP 800-30, Revision 1)"	"National Institute of Standards and Technology"	"Focuses exclusively on the information security risk assessment component of a holistic, organization-wide risk management process [NIS12a], [NIS12b]. Describes the basic concepts associated with assessing information security risk within organizations [NIS12a]. And it provides the process of assessing information security risk and guidance for the tasks pertaining to preparing for conducting, communicating findings, sharing risk-related information, and maintaining the risk assessment [NIS12a]. Appendices provide additional supporting risk assessment information including, among others, a taxonomy of threat sources (i.e., adversarial	Free of charge

Methodology Name	Publisher	Description	Access
		and non-adversarial), examples of threat events that could be initiated and of adverse impacts associated with threat events, qualitative and semi-quantitative sample assessment scales for threat source characteristics, vulnerabilities, likelihood of occurrence, impact of threat events, level of risk, along with sample templates for identification of threat sources, threat events (i.e., based on relevance), vulnerabilities, adverse impacts, and risk [NIS12a]" [Giu+21].	
"The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology, OCTAVE Allegro"	"Carnegie Mellon University Software Engineering Institute"	"Provides an information security risk assessment methodology pivoting on the containers of information assets to support the cybersecurity risk assessment process [SEI07]. The risk assessment process involves eight steps structured by means of four areas of activity illustrated using the OCTAVE Allegro roadmap, specifically establishing drivers where risk management criteria is defined based on the organization's objectives and impact areas are prioritized, profiling assets by creating a profile for the organization's information assets and identifying information asset containers, identifying threats through identification of areas of concern (i.e., real-life scenarios) and possible threat scenarios (their descriptions may include probabilities) along with their analysis, and identifying and mitigating risks by recording the corresponding consequence to an organization should a threat scenario materializes, computing the relative risk score (i.e., using a semi-quantitative method) considering the extent to which the consequence of a threat scenario affects the organization (i.e., the impact value) against the relative importance of the impact areas (i.e., the impact area rank), and selecting mitigation strategy for the risks that are unacceptable [SEI07]. Further guidance (Appendix A – OCTAVE Allegro Method Guidance v1.0), worksheets (Appendix B – OCTAVE Allegro Worksheets v1.0), and threat scenario questionnaires (i.e., Appendix C – OCTAVE Allegro Questionnaires v1.0) that support the process are provided in the appendices [SEI07]" [Giu+21].	Free of charge
"The Information Risk Assessment	"The Information Security Forum (ISF)"	"Describes a practical organization centric end-to-end risk-based information risk assessment methodology and provides pragmatic guidance on implementation and risk treatment [ISF14]"	Freely available to members

Methodology Name	Publisher	Description	Access
Methodology 2 (IRAM2)”		[Giu+21]. “IRAM2 process is structured using a six-phase assessment approach comprising 19 underpinning steps and key activities” [Giu+21]. “Thus, the methodology commences with the scoping phase to develop an environmental profile and define the scope of the exercise, then the business impact assessment is described to identify information assets and assess the organizational inherent impact should the CIA triad of these assets be compromised considering both realistic and worst-case scenarios. Next, the threat profiling phase is outlined by defining the threat landscape, categorizing threats and determining their characteristics, prioritizing threats, identifying threat events in-scope, and determine the assets impacted by threat events. Subsequently, the vulnerability assessment phase involves identifying the exploitable vulnerabilities and mapping related controls to vulnerabilities, evaluating the effectiveness of the controls, and establishing the control strength for each threat event and component pairing. Further, the risk evaluation phase aims to create a prioritized residual risk profile by deriving the residual risk rating from the residual likelihood of risk occurrence combined with the residual business impact rating for each risk, and plotting the two resulting risk factors on a residual risk matrix” [Giu+21]. “Finally, the risk treatment phase includes the evaluation of each risk against the organization’s risk appetite, the development of risk treatment options and plan with agreed and formally approved treatment actions, timelines and ownership, then execution of the risk treatment plan, and outcome validation to determine whether the residual risk ratings lie within the risk appetite and enable further treatment of any deviations, and ultimately the latest prioritized residual risk profile is continuously managed [ISF14]” [Giu+21].	
“CIS Risk Assessment Method (RAM) Version 1.0”	“Center for Internet Security (CIS)”	“Describes a process for conducting risk assessment projects and provides a risk assessment methodology (i.e., aligned with the Tiers as defined by the NIST Cybersecurity Framework) for organizations to adopt based on the characteristics of their approach to managing cybersecurity risk, along with guiding principles for assessing risks, three sets of instructions, exercises, templates (i.e., in the supplementary document	Free of charge

Methodology Name	Publisher	Description	Access
		CIS_RAM_Workbook), and examples to assist organizations while conducting risk assessments and designing control mechanisms based on the CIS Controls V7 [NIS18a], [CIS18b]. Thus, the activities from the risk assessment process which are generally applicable include: defining the assessment scope, scheduling interview sessions, setting risk assessment and acceptance criteria, gathering evidence, threat modelling, and evaluating risks, along with recommending and validating safeguards. Nevertheless, the focus (i.e., control-based, asset-based, threat-based), sequence, and complexity of activities and approach will vary depending on the profile (i.e., Tier 1, Tier 2, or Tier 3 and 4) to which the organization corresponds [CIS18b]. In this context, control-based implies mapping current controls to relevant CIS controls and conducting a control gap analysis to identify the assets susceptible to threats, asset-based refers to pairing the organization's information assets with the CIS controls to establishing whether current controls are appropriate, and threat-based alludes to commencing the risk analysis by means of attack path (i.e., aka kill chain) modelling, listing potential threats and corresponding information assets to identify misalignments between current controls and CIS Controls and determine the need for mitigating controls [CIS18b]" [Giu+21].	

Table 1.4. Overview of selected cybersecurity risk management methodology [Giu+21]

Methodology Name	Publisher	Description	Access
"Managing Information Security Risk: Organization, Missions and Information System View (NIST Special Publication 800-39)"	"National Institute of Standards and Technology"	"Outlines the components associated with managing information security risk following a multi-level approach (i.e., the information system, mission/business process, and organization levels) [NIS11]. And, it provides the process and life cycle of managing information security risk along with guidance for the tasks relating to framing risk (i.e., context setting for organization-wide risk-based decision making) to produce threat information and enable risk management strategy development, assessing risk to determine the organization's risk, responding to risk in accordance with the organizational risk frame, and ongoing risk monitoring and	Free of charge

Methodology Name	Publisher	Description	Access
		communications for continuous improvement of the organization's risk profile [NIS11], [NIS12b]. Appendices provide additional risk management related information including, among others, references and concepts, roles and responsibilities, process tasks, governance models, trust models, and risk response strategies [NIS11]" [Giu+21].	

Table 1.5. Overview of selected cybersecurity maturity assessment methodology [Giu+21]

Methodology Name	Publisher	Description	Access
"Cyber Resilience Review (CRR)"	"Carnegie Mellon University"	"Describes an end-to-end capability maturity assessment process for measuring the organization's cybersecurity resilience, and provides an interview-based methodology (i.e., consisting of 297 questions) for understanding the organization's cybersecurity practices in terms of service management and asset control and assessing the organization's cybersecurity management program relative to the NIST Cybersecurity Framework (CSF) (i.e., a crosswalk document that maps this methodology to the NIST CSF), by focusing on ten domains (i.e., asset management, controls management, configuration and change management, vulnerability management, incident management, service continuity management, risk management, external dependency management, training and awareness, and situational awareness) where each domain includes a set of goals with practice questions specific to the domain, and a standard set of Maturity Indicator Level (MIL) questions [Car16], [Dep18]. Thus, the three main phases of the assessment process include conducting the cyber resilience assessment, interpreting the resulting findings based on the organizational context, and determining the next actions for strengthening the organization's cybersecurity posture [Car16]. In addition, a process checklist for guiding the assessment is provided as part of appendices" [Giu+21].	Free of charge

1.1.2. Internet of Things (IoT): Background

The term "Internet of Things (IoT)" was coined in 1999 by the British technology pioneer Kevin Ashton and the first IoT device (i.e., an Internet-connected refrigerator) was announced by LG in 2000 [Als+19].

These days, from the perspective of the omnipresent digital transformation phenomenon, organizations from around the world leverage the technological advances and embrace cutting-edge technologies at an unprecedented velocity to enable intelligence-led decision-making, streamlined operations, customer-centricity, competitive advantage, and accelerate economic ascension [ENI18a], [EY18a], [Pop+18], [PwC17], [WEF18b], [Giu+21]. Based on the information disseminated by the author through the research paper [Pop+21b], the COVID-19 pandemic "has further fueled technical innovations and technological convergence, expedited digital connectivity in and around organizations, and made way for a greater international appetite towards remote everything (e.g., remote work, remote healthcare) [WEF21]" [Pop+21b]. In this context, "this pandemic arguably acted as a catalyst for greater critical dependency on internet-based technologies [WEF20a] including, inter alia, some of the Internet of Things (IoT) technologies" [Pop+21b]. For instance, throughout the COVID-19 pandemic, "IoT has been employed for predicting how the COVID-19 pandemic unfolds, tracking the health conditions of people, monitoring COVID-19 patients, tracking the real-time location of medical equipment, and detecting fraudulent healthcare insurance claims [Sin+20]" [Pop+21b]. Moreover, the application of IoT in healthcare was studied as part of a systematic review conducted by Kashani et al. (2021) [Kas+21], [Pop+21b]. Besides its application in healthcare, IoT has "various application areas, including smart mobility, smart grid, smart home / building, public safety and environment monitoring, industrial processing, smart agriculture, and independent living [Kha+20]" [Pop+21b]. Hence, based on the information disseminated by the author through the research paper [Pop+21b], "there are numerous research studies that cover individual and various application areas of IoT" [Pop+21b]. With respect to "the various application areas of IoT", examples of studies include "the comprehensive review conducted by Khanna and Kaur (2020) [Kha+20] that highlighted, among others, various contributions of researchers in different areas of applications of IoT", and "the comprehensive literature-based survey conducted by Hassan et al. (2020) [Has+20] that focused on exploring the applications of IoT in different areas, including healthcare, environmental, commercial, industrial, smart cities, and infrastructural applications" [Pop+21b]. Then, with respect to the "individual application areas of IoT", examples of studies include "the research works about an advanced IoT-based transportation system for efficient vehicle routing and scheduling in urban areas" that "described the concept and methodological approach for its development [Gay+18]", "proposed its architecture [Gay+20]", and "demonstrated its use in a case study [Kec+20]" [Pop+21b]. Thus, based on the information disseminated by the author through the research paper [Pop+21b], "the various application areas of IoT along with the numerous research contributions in different areas of applications of IoT indicate an extensive appetite for leveraging IoT technologies" [Pop+21b].

Furthermore, World Economic Forum (2020b) [WEF20b] anticipated "an even faster adoption of IoT technologies in the post COVID-19 economy" [Pop+21b]. The prospect of IoT growth over the next few years "was also highlighted in the study conducted by Khanna and Kaur (2020) [Kha+20]", which "pointed out that the need for greater interaction between various entities and more precise evaluation of sensor data are key drivers for ubiquitous connectivity" [Pop+21b].

Thus, "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" [Pop+21a]. 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" [Pop+21a]. For instance, the Ponemon Institute (2020) [Pon20] "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" [Pop+21a]. As part of the AT&T cybersecurity insights report, AT&T (2016) [AT&T16] "pointed out the rapid growth of connected IoT devices worldwide which resulted from the 500 individuals surveyed on the state of IoT security" [Pop+21a]. As part of the Congressional Research Service (CRS) report on IoT, CRS (2020) [CRS20] "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" [Pop+21a]. 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 [Del20]" [Pop+21a]. As highlighted by the International Electrotechnical Commission (IEC) (2016) [IEC16], "IoT has a significant impact on the global economy based on the IoT market forecasts of three worldwide well-renowned consulting firms" [Pop+21a]. As part of the Juniper Research's whitepaper on IoT, Juniper Research (2020) [Jun20] "provided a more aggressive projection for the total global number of IoT connections which could get to 83 billion by 2024" [Pop+21a]. According to Lee (2020) [Lee20], "an increasing number of IoT devices are connected" [Pop+21a]. "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 (2017) [McK17] "indicated this tendency as a key driver towards the massive rise of IoT" [Pop+21a]. McKinsey & Company (2019) [McK19] also "anticipated a steady growth of IoT investments and the increase of the worldwide number of IoT connected devices to 43 billion by 2023" [Pop+21a]. The prospects of IoT growth "were echoed by World Economic Forum (2020a) [WEF20a] which predicted 25 billion connected IoT devices globally by 2025" [Pop+21a]. As part of another insight report, "World Economic Forum (2020b) [WEF20b] increased their expectation from 25 billion connected devices worldwide to 41.6 billion and highlighted the investment growth surrounding IoT adoption" [Pop+21a].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21a], 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" [Pop+21a]. For example, CRS (2020) [CRS20] "pointed out that the deployment of 5G cellular networks and technologies will drive IoT growth" [Pop+21a]. Juniper Research (2020) [Jun20] "adopted a similar tone on the IoT growth indicating 5G as a key driver for IoT adoption" [Pop+21a]. With respect to "the perks of leveraging 5G technology", the World Economic Forum (2020a) [WEF20a] "indicated 5G as a core component of IoT as it enables greater speeds and reliability of communications for much more IoT devices" [Pop+21a]. According to McKinsey & Company's insights report, McKinsey & Company (2020a) [McK20a] "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" [Pop+21a].

Then, the remaining of this sub-subchapter focuses on defining and outlining some of the main IoT concepts.

1.1.2.1 Internet of Things (IoT) Concepts

"Internet of Things (IoT)" denotes "a system of interconnected homogeneous and/or heterogeneous systems and services that enable information processing and various interactions" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a], this definition of IoT "is derived from and based on the definitions from the CRS (2020) [CRS20], IEC (2016) [IEC16], and Garcia-Morchon et al. (2019) [Gar+19]" [Pop+21a]. In this sense, it is safe to say that "IoT is fundamental towards achieving ubiquitous connectivity in this era of digital transformation [WE20a], [Eur20], [HFS19]" [Pop+21a].

An IoT ecosystem includes components that correspond to different layers and the IoT reference model proposed by ITU-T [ITU12] (see Fig. 1.4) illustrates some of the main capabilities involved [Pop21].

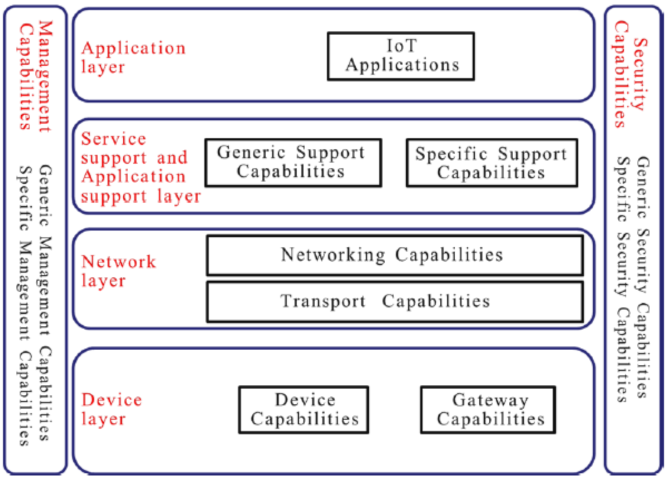

Management Capabilities
Generic Management Capabilities
Specific Management Capabilities
Application layer
IoT Applications
Service support and Application support layer
Generic Support Capabilities
Specific Support Capabilities
Network layer
Networking Capabilities
Transport Capabilities
Device layer
Device Capabilities
Gateway Capabilities
Security Capabilities
Generic Security Capabilities
Specific Security Capabilities

Fig. 1.4. IoT reference model [ITU12]

As depicted in Fig. 1.4, the IoT reference model consists of four layers (i.e., "device layer", "network layer", "service support and application support layer" and "the application layer") and two capabilities (i.e., "management capabilities" and "security capabilities") that span across all four layers [ITU12].

According to ITU-T, "the device layer" consists of two types of capabilities, namely [ITU12]:

- **"The device capabilities":** are introduced in the IoT reference model of ITU-T by providing examples of capabilities that address the interaction between devices and communication networks (i.e., direct interaction of devices with the communication network, indirect interaction of devices with the communication network through gateway capabilities and ad-hoc networking) and an energy saving capability (i.e., sleeping and waking-up mechanisms) [ITU12]. In addition, the IoT device capabilities involve the direct interaction of computing devices with the physical world through the transducer capabilities (i.e., sensing and actuating) [NIS19b]. While the sensing capabilities observe and measure an aspect of the physical world (e.g., temperature measurement, radiographic imaging, optical sensing, audio sensing), the actuating capabilities change something in the physical world based on previously processed information (e.g., heating coils, cardiac electric shock delivery, electronic door locks, servo motors) [ENI17b], [NIS19b]. At least one of these two transducer capabilities exists as part of an IoT device [NS19b].

- **"The gateway capabilities":** are introduced in the IoT reference model of ITU-T by providing some examples of multiple interfaces support and protocol conversion capabilities for both device to device interaction and device to network interaction when different protocols are used at the device layer and/or at the network layer [ITU12]. In a similar manner, NIST outlines the application interface capability for enabling device interactions at the device layer (e.g., application programming interface) and the network interface capabilities for enabling the device interactions with the communication network (e.g., Ethernet, Wi-Fi, Bluetooth, ZigBee) [NIS19b]. In addition, the human user interface capabilities (e.g., touch screens, cameras, microphones) are outlined by NIST for enabling the direct communication between IoT devices and people [NIS19b].

Then, "the network layer" consists of two types of capabilities, namely the "networking capabilities" (i.e., for controlling network connectivity) and "transport capabilities" (i.e., for ensuring connectivity for IoT data transport) [ITU12].

Afterwards, "the service support and application support layer" consists of two types of capabilities namely "the generic support capabilities" (i.e., to provide common support functions to different IoT applications) and "specific support capabilities" (i.e., to provide different support functions to different IoT applications) [ITU12].

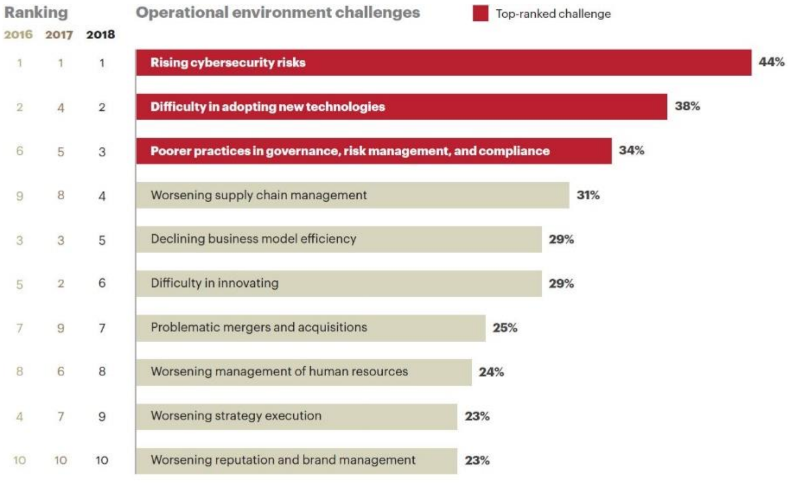
Subsequently, "the application layer" includes IoT applications [ITU12].

Then, "the management capabilities layer" consists of two types of capabilities, namely "the generic management capabilities" (e.g., device management, traffic congestion and management) and "specific management capabilities" (i.e., support application-specific requirements) [ITU12].

Finally, "the security capabilities layer" consists of two types of capabilities, namely "the generic security capabilities" (i.e., independent of applications) and "specific security capabilities" (i.e., support application-specific requirements) [ITU12].

1.2. The Motivation for the Doctoral Thesis

Nowadays, organizations aiming to achieve efficiencies and gain commercial advantage over competitors leverage the ubiquitous nature of cyberspace and engage in the digital transformation (DX) race, while operating in a risky business environment subject to rampant cyber threats, novel attack avenues, and tightened regulatory scrutiny [Jal+18], [Giu+21], [Pop+19b]. In this context, the „Views from the C-Suite" survey carried out worldwide by A.T. Kearney with 400 C-level executives and board members revealed that "the top three challenges faced by organizations are the rising cybersecurity risks, difficulty in adopting new technologies, and poor risk management practices (Fig. 1.5) [ATK18]" [Pop20].



Note: Numbers do not add up to 100 because respondents could select up to three choices.

Fig. 1.5. Top business operations challenges [ATK18]

Moreover, according to the World Economic Forum (2018b, 2019) [WEF18b], [WEF19] cyber risks are ever burgeoning, and are consolidating their position among the top ten global risks both in terms of probability of occurrence and of the corresponding consequence for individuals and for society including data theft, denial of critical services, disinformation spread, privacy loss, just to name a few [Pop+19b]. In this context, cyber defenders are striving to engineer and embrace more powerful ways of providing cyber readiness and resilience. Hence, the winners in the new DX race are those organizations that successfully adopt new technologies in an agile manner while navigating cybersecurity risk through sound cybersecurity risk management [ATK18]. Moreover, having a robust cybersecurity risk management strategy in place that guides and informs risk-based decisions for managing cybersecurity and privacy risks [NIS18b] is prerequisite for organizations that aim to effectively address cybersecurity risk [NIS11]. Notwithstanding, the prevalent cybersecurity strategies have not moved enough towards becoming more proactive [Nat17], [ATK18], [Pon19], [EY20]. Thus, current cybersecurity risk management practices are not adequate enough, and this issue has its roots in a poor establishment of the organizational understanding for managing cybersecurity risk within organizations. Consequently, this issue has significant implications on organizations, which may include hampering their ability to effectively defend against hostile cyber offenders that are incessantly innovating and proliferating powerful ways of breaking cybersecurity mechanisms, hindering the ability of these organizations to successfully navigate cybersecurity compliance requirements, and hamstring their ability to securely onboard new technologies.

Furthermore, with respect to the challenge related to the difficulty in adopting new technologies, the study conducted by A.T. Kearney (2018) [ATK18] revealed that the adoption of the Internet of Things (IoT) is a top challenge in technology adoption. In addition, according to McKinsey & Company (2017) [McK17], cybersecurity is more relevant and challenging than ever due to the rise of IoT. Moreover, a study of World Economic Forum (2020a) [WEF20a] indicated the IoT as one of four transformative technologies (i.e., IoT, artificial intelligence, quantum computing, next-generation approaches to identity and access management) representative to illuminate the range of cybersecurity risk for the next 5–10 years.

In this context, "numerous entities around the globe are working on developing mandatory and voluntary IoT security requirements aimed at stimulating industry and government organizations to adopt robust IoT security practices" [Pop+19b]. Hence, based on the information disseminated by the author through the research paper [Pop+21b], "on top of the existing cybersecurity-related laws and regulations [Pop+19a], government and regulatory bodies from around the world work on introducing new laws to increase IoT security" [Pop+19b]. For instance, "the US Congress [USC20] enacted the federal IoT Cybersecurity Improvement Act of 2020, which aims to establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes", and "the UK's Department for Digital, Culture, Media & Sport [DCM21] plans to introduce new laws that regulate the security of consumer IoT devices" [Pop+19b]. Moreover, in response to the IoT security issues and risk, "domestic and international standards bodies and industry associations have developed various IoT security codes of practice, standards, guidelines, and frameworks [Pop+21a]" [Pop+19b].

Notwithstanding, "the current state of risk management for IoT is far behind the target state" [Pop+21a]. Hence, the Ponemon Institute (2020) [Pon20] "underlined the burning need to place IoT risk management improvement high on the agenda" [Pop+21a]. A.T. Kearney (2019) [ATK19] "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" [Pop+21a]. As part of Deloitte's report on IoT, Deloitte (2020) [Del20] "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" [Pop+21a]. World Economic Forum (2020b) [WEF20b] "pointed out immature IoT risk management capabilities, which may lead to poor IoT risk management practices" [Pop+21a]. According to Bain (2018) [Bai18], "the majority of the 280 executives surveyed indicated a great level of concern around the IoT risks to which their organizations are exposed" [Pop+21a].

In the context of managing IoT risk, based on the information disseminated by the author through the research paper [Pop+21a], "cybersecurity related issues give rise to the greatest level of concern, and cybersecurity is regarded as pivotal for organizations". For instance, IEC (2016) [IEC16] "named security, trust, privacy, and identity management among the key limitations and deficiencies of today's IoT" [Pop+21a]. As part of the World Economic Forum's report on the global state of IoT, World Economic Forum (2020b) [WEF20b] "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" [Pop+21a]. 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 [McK20b]" [Pop+21a]. As part of the AT&T cybersecurity insights report, AT&T (2016) [AT&T16] "claimed that IoT security is the top concern of the Chief Executive Officer's (CEO) agenda" [Pop+21a]. According to the findings from the study conducted by McKinsey & Company (2017) [McK17], "75% of the 400 IoT experts surveyed indicated IoT security as either important or very important" [Pop+21a]. As per the findings of Bain (2018) [Bai18], "the more mature are the organizations in terms of their cybersecurity capabilities, the more importance they place on their IoT risks" [Pop+21a].

Hence, based on the information disseminated by the author through the research paper [Pop+21a], "IoT security risk management may raise the greatest level of concern among organizations as there is no general IoT security model [IEC16], there is no global IoT security standard [WEF20b], there are only a few IoT security standards [McK17], and most best practices are not focused on IoT security risk management [Lee20], [WEF20a]" [Pop+21a]. Moreover, "cybersecurity strategies tend to be developed reactively rather than proactively in the transformation journey [EY20], [WEF20b], [Nat17]" [Pop+21a]. In this context, "it is very likely that, amid adopting IoT, many organizations out there lack adequate IoT security risk management strategies" [Pop+21a]. For instance, Lee (2020) [Lee20] "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" [Pop+21a]. The lack of cybersecurity strategies that cover IoT "was also pointed out by McKinsey & Company for a fairly considerable number of organizations [McK17]" [Pop+21a].

In this context, Fig. 1.6 examplifies how cybersecurity, cybersecurity risk management, IoT security, and IoT security risk management topics fit together, and highlights the topics of interest of this thesis (i.e., cybersecurity risk management and IoT security risk management).

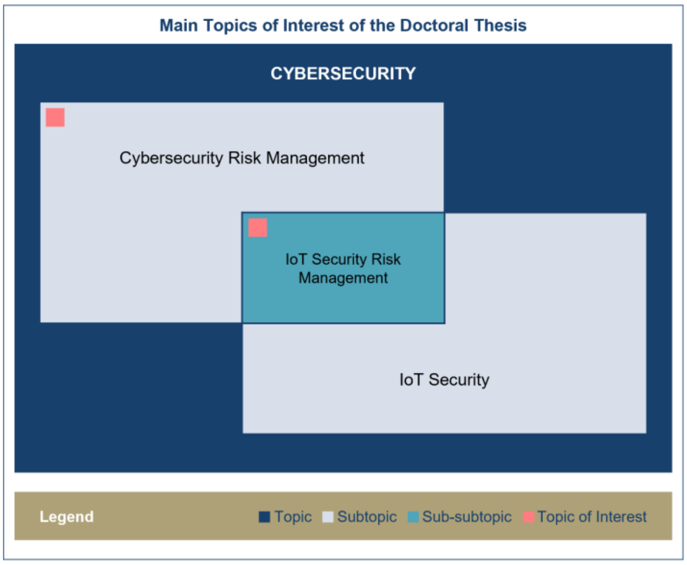

Main Topics of Interest of the Doctoral Thesis
CYBERSECURITY
Cybersecurity Risk Management
IoT Security Risk Management
IoT Security
Legend
Topic
Subtopic
Sub-subtopic
Topic of Interest

Fig. 1.6. Topics of interest of the doctoral thesis

Therefore, given the prevalence of reactive cybersecurity strategies [Nat17], considering that cybersecurity is more challenging than ever due to the rise of IoT security concerns [McK17], and taking into account the widespread "absence of robust IoT security risk management strategies in organizations" [Pop+21a], this thesis focuses on making contributions to the establishment of the organizational understanding for managing cybersecurity risk, and it focuses on bringing contributions to the establishment of the organizational understanding for managing the IoT security risk from the broader cybersecurity risk. Thus, this thesis aims to support cybersecurity practitioners to formulate or rethink their cybersecurity-related risk management strategies in advance of future cyber attacks. In view of this, Fig. 1.7 shows the four focus areas of this doctoral thesis by highlighting the key drivers of and enablers for cybersecurity risk management that are addressed.

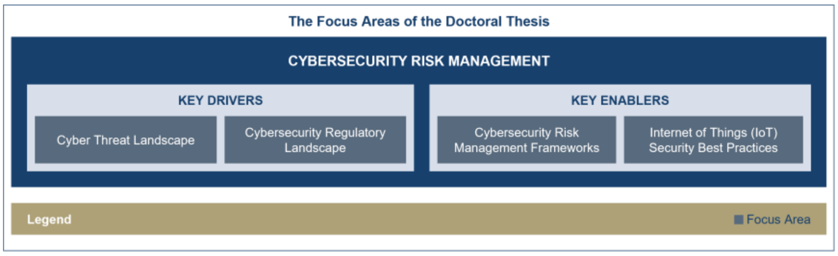

The Focus Areas of the Doctoral Thesis
CYBERSECURITY RISK MANAGEMENT
KEY DRIVERS
Cyber Threat Landscape
Cybersecurity Regulatory Landscape
KEY ENABLERS
Cybersecurity Risk Management Frameworks
Internet of Things (IoT) Security Best Practices
Legend
■ Focus Area

Fig. 1.7. Focus areas of the doctoral thesis

Furthermore, the rationale behind focusing on key drivers and enablers is provided below.

First, given that the strategic analysis (e.g., general enviromental analysis, company analysis, customer and market analysis, competition analysis) is of decisive importance to strategy development [Sch87], this thesis aims to facilitate the strategic analysis for organizations looking to frame or reframe their cybersecurity risk management strategy. Moreover, taking into account that this study targets a wide range of various organizations, this thesis focuses on the key drivers for cybersecurity risk management within organizations, namely the cyber threat landscape and cybersecurity regulatory landscape.

Second, given that the selection of cybersecurity-related best practices (e.g., frameworks, standards, guidelines) is essential for establishing the overall approach to cybersecurity that encompasses cybersecurity risk management [Net19] and that making use of planning instruments enable the creation of actionable strategies [Sch87], this thesis aims to facilitate the planning process for organizations looking to enhance their cybersecurity-related risk management strategies. Moreover, given that the selection of cybersecurity risk management frameworks is essential for developing a cybersecurity risk management strategy as these frameworks guide the approach to cybersecurity [Net19], this thesis focuses on these key enablers for cybersecurity risk management, namely the cybersecurity risk management frameworks. In addition, given that relying on IoT security best practices boosts the ratio of benefit to effort when crafting an IoT security risk management strategy, this thesis focuses on these key enablers for the IoT security risk management and the wider cybersecurity risk management, namely the IoT security best practices.

Moreover, the rationale behind focusing this doctoral thesis on the four focus areas (see Fig. 1.7) is provided below along with the corresponding thesis objectives.

Thus, with respect to the cyber threat landscape, the threat environment is ever evolving as the omnipresent digital transformation expands "the attack surface of modern organizations through infusion of complexity and diversification of attack avenues" that can be harnessed by diverse cyber threat actors [Ali+14], [Cra18], [ENI18a], [Pop+18], [PwC16], [PwC18], [Giu+21]. In this context, research work covering the current cyber threat landscape is required on ongoing basis considering the ever-changing nature of cyber threats and taking into account that organizations need to gain a true picture of the threat environment prior to framing a cybersecurity strategy [Net19]. Therefore, one objective of my thesis is to provide an overview of the current cybersecurity threats of organizations by carrying out a research work on the literature related to current cyber threat landscape. This study aims to enrich the current literature and should allow organizations to better grasp their inherent exposures and those stemming from their DX journey. Moreover, given that the existing cyber threat rating methods are characterized by high complexity or uncertainty [NIS12a], [OWA19], there is a need for a cyber threat rating method that is dissociated from elements that induce uncertainty and that fosters unbiased outputs in a more consistent manner by focusing on the possible extent of cyber harm that applies to the cyber threats. Thus, another objective of my thesis is to propose a cyber threat rating method that aims to reduce the complexity and uncertainty attached to the existing threat rating methods, and to prioritize current cyber threats using this proposed method.

Furthermore, with respect to the cybersecurity-related regulatory landscape, the global cybersecurity regulatory ecosystem not only entangles organizations in an intricate web of legislations and regulations but also is ever-changing, which makes harder for organizations doing business in one or multiple jurisdictions to achieving greater compliance with regulatory requirements to avoid the rising sanctions for law infringements and money draining litigations [Mar17], [May18], [Pon18], [Giu+21]. In this context, given the dynamic nature of the cybersecurity regulatory landscape, research work around key cybersecurity-related laws and regulations is needed and should be praised by fellow researchers and organizations that are keen to establish their cybersecurity compliance requirements in an optimized fashion. Hence, one objective of my thesis is to provide an overview of the cybersecurity regulatory landscape focused on key cybersecurity-related legislations and regulations from key cybersecurity jurisdictions by carrying out a research work on the literature related to current generally applicable cybersecurity-related laws and regulations pertaining to selected areas of statute and jurisdictions. Besides, given that compliance with applicable legislations can be a daunting and costly endeavor for organizations as some emerging legal requirements are converging with the existent ones inflicting organization-wide duplication, while others are inducing discrepancies that need to be carefully navigated depending on the organizational context [Del17a], [Mar17], [Pop+19a], there is a need for research works that explore cybersecurity-related legislations and regulations in relation to each other to alleviate the degree of complexity associated with attaining cybersecurity regulatory compliance. Hence, another objective of my thesis is to propose a method for evaluating key cybersecurity-related legislations from the perspective of the organizational understanding to managing cybersecurity risk to establish the degree of commonality between them, and to provide a critical evaluation of in-scope cybersecurity-related legislations based on the proposed method.

Furthermore, with respect to the cybersecurity risk management frameworks, standardization bodies and multiple other structures have recognized the need for greater cyber resilience and have reacted by promoting sound cybersecurity practices within organizations through various means including, among others, the development of cybersecurity-related frameworks, standards, voluntary guidance, and other best practices that can help organizations to enhance their cybersecurity strategy and security postures [May18], [Giu+21]. In addition, given that much of the literature up to now has outlined these frameworks, standards, and methodologies without clearly delineating the distinction between them [Twe+18], research work on the cybersecurity risk management frameworks is needed and should be welcomed by fellow researchers and organizations that wish to find out the cybersecurity risk management framework options in a streamlined manner. Hence, one objective of my thesis is to provide an overview of several well-renowned cybersecurity risk management frameworks. Moreover, considering that there is no universally accepted framework for managing cybersecurity risks as the work is often carried out in silos [Twe+18] and given that there are various cybersecurity-related frameworks in the literature that "can be leveraged by organizations, where each framework provides specific guidance and best practice applicable to one or more domains" [Cro13], [ENI06], [Ion13], [Tau14], [WIS16], [Giu+21], research works that provide comprehensive characterization of some of these frameworks relative to each other are deemed necessary and should be welcomed by fellow researchers and all organizations looking to understand some of the key features of these frameworks and/or to select the one most fit for their intended purpose. Hence, another objective of my thesis is to propose a methodology for evaluating cybersecurity risk management frameworks and to provide a critical evaluation of in-scope cybersecurity risk management frameworks based on the proposed methodology.

Finally, with respect to the IoT security best practices, "there are numerous best practices in the literature relevant to IoT security" and on top of this these best practices are not classified based on their applicability and type. In this context, there is a need for research works that explore and classify IoT security best practices [Pop+21a]. Therefore, one objective of my thesis is to provide an overview of the IoT security best practices and to classify these best practices using a proposed taxonomic hierarchy. Moreover, given "the prevalent absence of robust IoT security risk management strategies in organizations and the paucity of reference sources for IoT security risk management strategy", there is a clear need for an IoT security risk management strategy reference model [Pop+21a]. Thus, another objective of my thesis is to propose a methodology for developing an IoT security risk management strategy reference model, to propose the IoT security risk management strategy reference model, and to evaluate the proposed IoT security risk management strategy reference model against the IoT security best practices that are the most relevant for the proposed model. Moreover, given that the current literature has not focused on exploring "the current state of IoT security risk management strategies in organizations", there is a clear need for research works that address this aspect. Hence, the last objective of my thesis is to propose a methodology for undertaking a survey study to determine the current state of IoT security risk management strategies in the surveyed organizations relative to the proposed reference model for IoT security risk management strategy, to conduct the survey study based on the proposed methodology, and to report the survey findings based on the proposed methodology.

In summary, the need for tackling the top three challenges faced by organizations (i.e., "the rising cybersecurity risks", "difficulty in adopting new technologies", and "poor risk management practices") [ATK18], motivates the objectives of this doctoral thesis.

1.3. The Objectives of the Doctoral Thesis

Given that more research work is needed to enable organizations to better understand the key drivers of cybersecurity risk management, and to make more informed decisions when it comes to leveraging cybersecurity-related risk management enablers, this thesis focuses on making contributions to the establishment of the organizational understanding for managing cybersecurity risk, and it focuses on bringing contributions to the establishment of the organizational understanding for managing the IoT security risk from the broader cybersecurity risk. Thus, the objectives of my doctoral thesis are enumerated below:

- **Objective 1:** Provide an overview of the current cybersecurity threats of organizations;
- **Objective 2:** Provide an overview of the cybersecurity regulatory landscape focused on key cybersecurity-related legislations and regulations from key cybersecurity jurisdictions;
- **Objective 3:** Provide an overview of several well-renowned cybersecurity risk management frameworks;
- **Objective 4:** Provide an overview of the IoT security best practices and classify these best practices using a proposed taxonomic hierarchy;
- **Objective 5:** Propose a cyber threat rating method that aims to reduce the complexity and uncertainty attached to the existing threat rating methods and prioritize current cyber threats using this proposed method;
- **Objective 6:** Propose a method for evaluating key cybersecurity-related legislations to establish the degree of commonality between them from the perspective of the organizational understanding to managing cybersecurity risk and provide a critical evaluation of in-scope cybersecurity-related legislations based on the proposed method;
- **Objective 7:** Propose a methodology for evaluating cybersecurity risk management frameworks and provide a critical evaluation of in-scope cybersecurity risk management frameworks based on the proposed methodology;
- **Objective 8:** Propose a methodology for developing a reference model for IoT security risk management strategy, propose the IoT security risk management strategy reference model (IoTSRM2), and evaluate the proposed IoTSRM2 against the IoT security best practices that are the most relevant for the proposed model;
- **Objective 9:** Propose a methodology for undertaking a survey study to determine the current state of IoT security risk management strategies in the surveyed organizations relative to the proposed IoTSRM2, conduct the survey study based on the proposed methodology, and report the survey findings based on the proposed methodology.

Furthermore, Fig. 1.8 shows the objectives of my doctoral thesis mapped against the focus areas of my doctoral thesis.

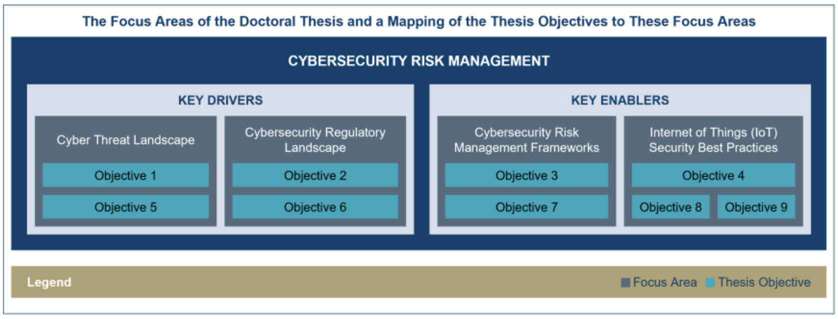

The Focus Areas of the Doctoral Thesis and a Mapping of the Thesis Objectives to These Focus Areas
CYBERSECURITY RISK MANAGEMENT
KEY DRIVERS
KEY ENABLERS
Cyber Threat Landscape
Objective 1
Objective 5
Cybersecurity Regulatory Landscape
Objective 2
Objective 6
Cybersecurity Risk Management Frameworks
Objective 3
Objective 7
Internet of Things (IoT) Security Best Practices
Objective 4
Objective 8
Objective 9
Legend
■ Focus Area
■ Thesis Objective

Fig. 1.8. The mapping of the thesis objectives to the focus areas of the doctoral thesis

1.4. The Structure of the Doctoral Thesis

This doctoral thesis is structured in seven chapters. **Chapter 1** represents the introductory chapter of this thesis, and it includes the background of, motivation for, and structure of the doctoral thesis.

Then, **Chapter 2** presents the overviews of the key drivers of and enablers for cybersecurity risk management. The overview of the key drivers of cybersecurity risk management comprises the overview of the cyber threat landscape and the overview of the cybersecurity regulatory landscape. Then, the overview of the key enablers for cybersecurity risk management comprises the overview of the cybersecurity risk management frameworks and the overview of IoT security best practices.

Afterwards, **Chapter 3** provides the evaluation of the key cybersecurity risk management drivers. This evaluation comprises the application of a proposed cyber threat rating method to evaluate cyber threats and the evaluation of cybersecurity-related legislations based on the proposed evaluation method.

Subsequently, **Chapter 4** contains the description of the proposed methodology for evaluating the in-scope cybersecurity risk management frameworks, the critical evaluation of the in-scope cybersecurity risk management frameworks based on the proposed methodology, and the analysis of related work relevant to the evaluation of cybersecurity risk management frameworks.

Then, **Chapter 5** includes the description of the proposed methodology for developing the IoT Security Risk Management Strategy Reference Model (IoTSRM2), the description of the proposed IoTSRM2, the critical evaluation of selected IoT security best practices in relation to the IoTSRM2, and the comparative analysis of the related work for the IoTSRM2 based on eight evaluation criteria.

Later, **Chapter 6** consists of the presentation of the research questions for the IoTSRM2-based survey study, the description of the proposed methodology for the IoTSRM2-based survey, the reporting of the results from conducting the IoTSRM2-based survey, and the comparative analysis of the related work for the IoTSRM2-based survey study using seven evaluation criteria.

Finally, **Chapter 7** draws the concluding remarks of the thesis, including the thesis contributions and the proposed future work.

Furthemore, Fig. 1.9 shows the structure of this thesis, maps the thesis objectives to the thesis chapters and/or subchapters where they are achieved, and provides a reading map for the thesis objectives. With respect to the reading map, this mapping should be leveraged in conjunction with the nine objectives of this thesis by readers interested in specific thesis objectives, where:

- **"Mapping 1"** corresponds to the outputs of my research work on the cyber threat landscape, which concretized in the achievement of the Objective 1 and Objective 5;
- **"Mapping 2"** corresponds to the outputs of my research work on the cybersecurity regulatory landscape, which concretized in the achievement of the Objective 2 and Objective 6;
- **"Mapping 3"** corresponds to the outputs of my research work on the cybersecurity risk management frameworks, which concretized in the achievement of the Objective 3 and Objective 7;

- **"Mapping 4"** corresponds to the outputs of my research work on the IoT security best practices, which concretized in the achievement of the Objective 4, Objective 8, and Objective 9.

For instance, assuming a reader is interested in Objective 9, Fig. 1.9 guides the reader via "Mapping 4" to read Chapters 1, 2.4, 5, 6, and 7.

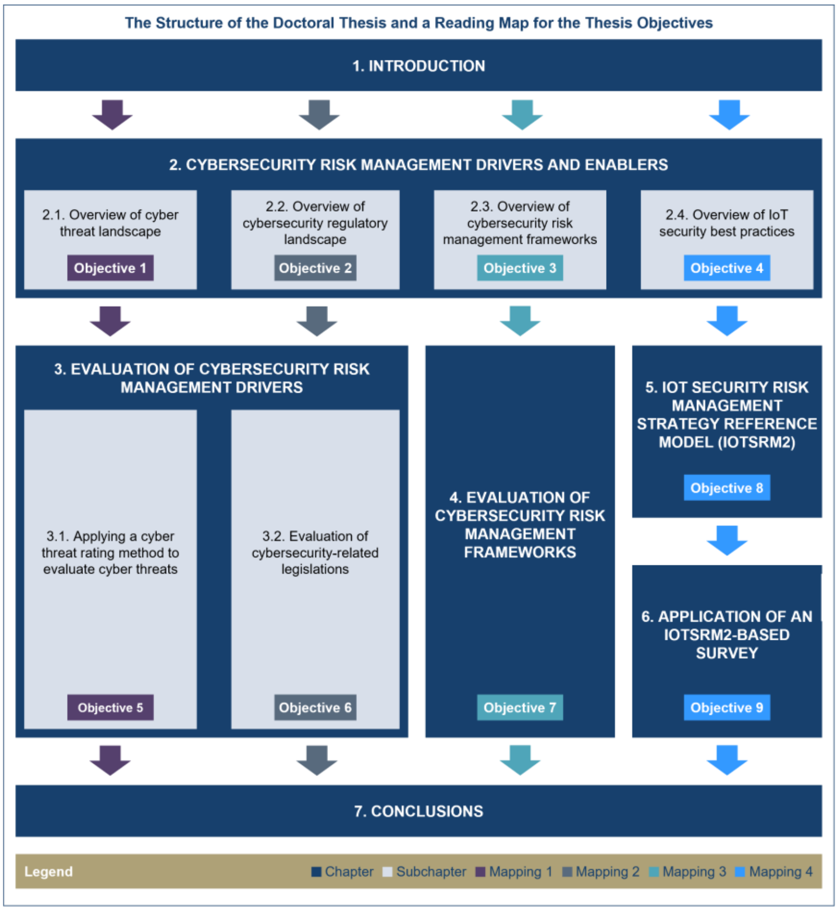

The Structure of the Doctoral Thesis and a Reading Map for the Thesis Objectives
1. INTRODUCTION
2. CYBERSECURITY RISK MANAGEMENT DRIVERS AND ENABLERS
2.1. Overview of cyber threat landscape
Objective 1
2.2. Overview of cybersecurity regulatory landscape
Objective 2
2.3. Overview of cybersecurity risk management frameworks
Objective 3
2.4. Overview of IoT security best practices
Objective 4
3. EVALUATION OF CYBERSECURITY RISK MANAGEMENT DRIVERS
3.1. Applying a cyber threat rating method to evaluate cyber threats
Objective 5
3.2. Evaluation of cybersecurity-related legislations
Objective 6
4. EVALUATION OF CYBERSECURITY RISK MANAGEMENT FRAMEWORKS
Objective 7
5. IOT SECURITY RISK MANAGEMENT STRATEGY REFERENCE MODEL (IOTSRM2)
Objective 8
6. APPLICATION OF AN IOTSRM2-BASED SURVEY
Objective 9
7. CONCLUSIONS
Legend
■ Chapter ■ Subchapter ■ Mapping 1 ■ Mapping 2 ■ Mapping 3 ■ Mapping 4

Fig. 1.9. The thesis structure and a reading map for the thesis objectives

2. CYBERSECURITY RISK MANAGEMENT DRIVERS AND ENABLERS

This chapter provides overviews of the key drivers of and enablers for cybersecurity risk management. With respect to the key drivers, first, the chapter provides an overview of the cyber threats in the current digital transformation age, and then it provides an overview of the cybersecurity-related legislations and regulations pertaining to selected areas of statute under selected jurisdictions. Subsequently, about the enablers, first, the chapter provides an overview of cybersecurity risk management frameworks and then the chapter provides an overview of some of the most well-renowned IoT security best practices.

These overviews aim to present the current state of the cyber threat landscape, cybersecurity regulatory landscape, cybersecurity risk management frameworks, and IoT security best practices, and to pinpoint needs for improvement in each of these four areas. Furthermore, these overviews aim to enable the advancement of this doctoral research via the delivery of further contributions in the next chapters of this thesis.

Thus, this chapter addresses the following four thesis objectives:

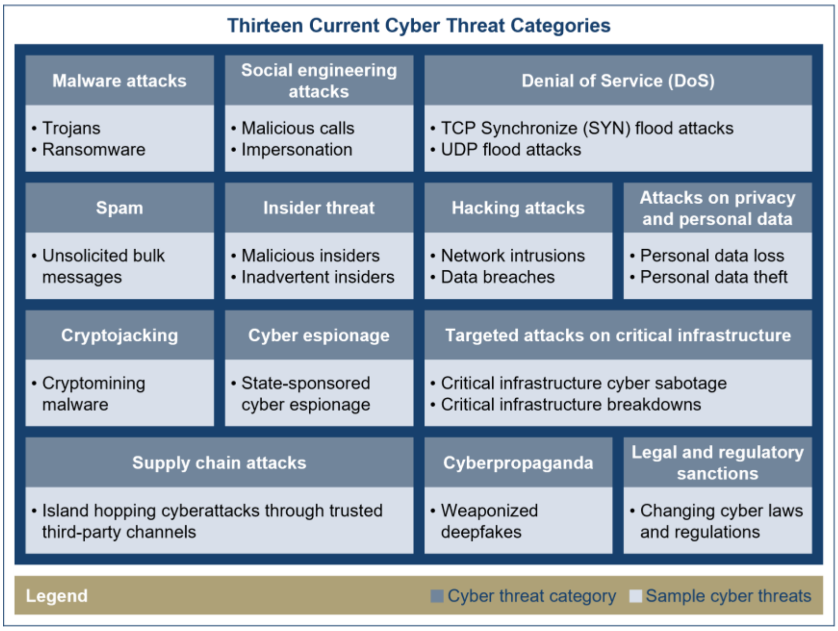
- **Objective 1:** Provide an overview of the current cybersecurity threats of organizations;
- **Objective 2:** Provide an overview of the cybersecurity regulatory landscape focused on key cybersecurity-related legislations and regulations from key cybersecurity jurisdictions;
- **Objective 3:** Provide an overview of several well-renowned cybersecurity risk management frameworks;
- **Objective 4:** Provide an overview of the IoT security best practices and classify these best practices using a proposed taxonomic hierarchy.

2.1. Overview of Cyber Threat Landscape

Based on the information disseminated by the author through the research paper [Pop+19b], cyber risk assessment activities rely either on comprehensive threat taxonomies developed to achieve a high degree of threat completeness [Lau18], or on threat modelling methods that come with pre-built high-level cyber threat categories [She+18]. In this context, there are numerous threat taxonomies including, among others, Open Threat Taxonomies (OTT) [Tar+15], ENISA Threat Taxonomy (ETT) [ENI16b], NIST Risk Assessment Threat Exemplary [NIS12a], Taxonomy of Operational Cyber Security Risks (TOCSR) [Ceb+14], [Lau18], and the Cyber Threat Taxonomy proposed by Ferdinand and Benham (2017) [Fer+17]. Besides, there are specific threat categories based on a set of known threats (e.g., "spoofing identity, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege") that come with threat modelling methods, such as STRIDE which proved to have a moderately high rate of false negatives [She+18]. Thus, instead of proposing a novel threat taxonomy and aiming to achieve a higher level of threat completeness, this subchapter provides a catalog of some of the most up-to-date categories of cyber threats drawn from reviewed sources with the purpose of reducing the complexity attached to carrying out cybersecurity risk assessments within organizations, keeping pace with the ever-evolving cyber threat landscape, and focusing on the organizational rather than national level. Additionally, through the selected threat categories this chapter aims to reduce the false negatives that might be introduced by the cyber threat categories corresponding to some of the existing threat modelling methods (e.g., STRIDE) [She+18], [Pop+19b]. In this sense, based on the information disseminated by the author through the research paper [Pop+19b], for creating the catalog with the most recent threat categories, seventeen relevant and well-renowned sources were analyzed, including the following [Pop+19b]:

- Threat landscape reports from Accenture (2018) [Acc18], Booz Allen Hamilton (2019) [Boo19], ENISA (2019a) [ENI19a], GSMA (2019) [GSM19], IBM (2019) [IBM19], Oracle (2019) [Ora19], Symantec (2019) [Sym19], Thales (2018) [Tha18], and WEF (2019) [WEF19];
- Survey reports from Crown (2019) [Cro19] and NCSC (2018) [NCS18] covering cybersecurity incidents or data breaches in the United Kingdom;
- A law enforcement report from Europol (2018) [Eur18] covering cybercrime;
- A survey report from EY (2018b) [EY18b] covering the global state of cybersecurity;
- An insight report from KPMG (2019) [KPM19] covering key cybersecurity considerations;
- Insight reports from Secureworks (2019) [Sec19] and Verizon (2019) [Ver19] covering incident response insights, data breaches investigations;
- A trend report from Trend Micro (2018) [Tre18] covering security predictions.

Hence, based on the information disseminated by the author through the research paper [Pop+19b], this subchapter provides an overview of the current cyber threats by consolidating and categorizing the most frequently encountered cyber security threats and by outlining the identified cyber threat categories based on the analysis of the seventeen selected sources. Thus, following the analysis of the current security incidents and threats from the aforementioned reports, the selected cyber threat categories encompass "malware attacks", "social engineering attacks", "denial of service (DoS)", "spam", "insider threat", "hacking attacks", "attacks on privacy and personal data", "cryptojacking", "cyber espionage", "targeted attacks on critical infrastructure", "supply chain attacks", "cyberpropaganda", and "legal and regulatory sanctions" [Pop+19b]. Fig. 2.1 shows the thirteen cyber threat categories together with a few examples of relevant cyber threats.



Thirteen Current Cyber Threat Categories

Malware attacks
- Trojans
- Ransomware

Social engineering attacks
- Malicious calls
- Impersonation

Denial of Service (DoS)
- TCP Synchronize (SYN) flood attacks
- UDP flood attacks

Spam
- Unsolicited bulk messages

Insider threat
- Malicious insiders
- Inadvertent insiders

Hacking attacks
- Network intrusions
- Data breaches

Attacks on privacy and personal data
- Personal data loss
- Personal data theft

Cryptojacking
- Cryptomining malware

Cyber espionage
- State-sponsored cyber espionage

Targeted attacks on critical infrastructure
- Critical infrastructure cyber sabotage
- Critical infrastructure breakdowns

Supply chain attacks
- Island hopping cyberattacks through trusted third-party channels

Cyberpropaganda
- Weaponized deepfakes

Legal and regulatory sanctions
- Changing cyber laws and regulations

Legend ■ Cyber threat category □ Sample cyber threats

Fig. 2.1. Proposed cyber threat categories with examples of cyber threats

Furthermore, based on the information disseminated by the author through the research paper [Pop+19b], these thirteen cyber threat categories are described below.

"Malware attacks" rely on malicious code (e.g., viruses, worms, trojans, ransomware, spyware) and leverage exploitable vulnerabilities to circumvent cybersecurity mechanisms and carry out unauthorized or adversarial undertakings that may harm the confidentiality, integrity, and availability of information systems [NIS19a]. Nowadays, malware-driven intrusions are the most prevalent category of cyber threats [ENI19a]. Hence, some of the key malware threats include ransomware (e.g., "WannaCry", "NotPetya"), banking trojans (e.g., "Emotet", "Trickbot"), and living off the land (e.g., malicious use of PowerShell). About ransomware, this remains a prominent malware threat and infamous extortion tool despite the recent decline in the number of reported incidents [Acc18], [ENI19a], [Eur18], [Sec19], [Sym19], [Ver19]. Also, even though according to Europol (2018) [Eur18] the number of banking trojans infections is dropping, they continue to pose significant threats to consumers [ENI19a], [IBM19], [Sym19], [Ver19]. And, with respect to living off the land techniques, these cyberattacks are more and more widespread as they enable greater obfuscation capabilities to bypass security controls [ENI19a], [IBM19], [Sym19], [Pop+19b].

"Social engineering attacks" are using manipulation techniques as part of scams via fraudulent messages, malicious calls, or impersonation by means of different channels such as emails, mobile phones, social media, or physical means [Cro19], [ENI19a], [EY18b]. Victims are lured by attackers to reveal sensitive information (e.g., credentials, cardholder data) or to engage in harmful activities (e.g., running malicious files, clicking on unsafe links) without knowing [ENI19a], [Lon+13a], [NCS18], [NIS19a]. One of the most common technique used by attackers is spam-related phishing, however targeted phishing attacks such as spear-phishing or Business Email Compromise (BEC) also known as whaling attack or "CEO fraud" continue to mount and to record greater financial losses for organizations [ENI19a], [IBM19], [NCS18], [Ora19], [Sym19]. Also, victims might be tricked via masquerading calls (i.e., vishing), fraudulent Short Message Service (i.e., smishing), fraudulent websites, phishing through electronic messaging systems (e.g., mobile messaging, social media) or physical means (i.e., impersonation) [Cro19], [ENI19a], [Pop+19b].

"Denial of Service (DoS)" attacks are making networks and systems unavailable for authorized users by overwhelming the victim's resources [Lon+13b], [NIS19a], [Ver19]. Over the years, DoS attacks have caused significant harm to organizations leading to service disruption or performance degradation [Cro19], [ENI19a], [NIS19a]. Examples of DoS attacks include "Transfer Control Protocol (TCP) Synchronize (SYN) flood attacks", "User Datagram Protocol (UDP) flood attacks", "Internet Control Message Protocol (ICMP) flood attack", and "Border Gateway Protocol (BGP) rerouting" [ENI19a], [IBM19]. In addition, resources might get overloaded from distributed locations using botnets (e.g., Mirai, Aidra, Wifatch) for launching Distributed Denial of Service (DDoS) attacks [IBM19], [Sym19]. Nowadays, organizations are experiencing a surge of DDoS attacks due to the proliferation of unsecured Internet of Things (IoT) devices [ENI19a], [NCS18], [Pop+19b].

"Spam" attacks abuse the electronic messaging systems and flood victims with unsolicited messages sent in bulk [ENI19a], [NIS19a]. These unwanted bulk messages not only consume network bandwidth and storage resources but may also contain malicious links and attachments which could confer an initial foothold on the victim's network or facilitate scams [ENI19a], [Eur18], [IBM19]. Hence, currently spam is among the top ten cyber threats faced by organizations [EY18b]. And, with respect to the current spam activity, even though some data indicates a steady decrease in spam over the last years [ENI19a], [Tru18], other data reveals that there has been an increase in the spam rates since 2015 [Sym19], [Pop+19b].

"Insider threat" is one of the major threats performed by insiders (e.g., employees, privileged IT users, contractors), which may cause inadvertent or malicious harm (e.g., financial, operational, and reputational) by compromising "the confidentiality, integrity, or availability" of the victim's information assets [ENI19a], [GSM19], [IBM19], [Sec19]. With respect to inadvertent insiders, they may cause various security issues (e.g., disclosure of sensitive information, data loss) by falling for social engineering attacks, using shadow IT, or being careless about sound cybersecurity practices among others [ENI19a], [GSM19], [IBM19], [Ora19]. In addition, malicious insiders (e.g., IT administrators) are ranked among some of the key data security threats according to Thales (2018) [Tha18] Data Threat Report Survey [Pop+19b].

"Hacking attacks" aim to gain unauthorized access to information systems, move laterally, steal money or data, and maintain presence inside or sabotage organizations [NIS19a], [WEF19]. These days, network intrusions are mostly driven by theft of data which is used by cyber criminals to commit fraudulent activities (e.g., extortion, card not present fraud) [ENI19a], [Eur18], [EY18b], [WEF19]. Thus, with respect to data breaches, hacking attacks are the most prevalent threat category [Ver19]. And successful hacking activities mainly rely on leaked or stolen credentials, backdoors, or lax cybersecurity such as ad hoc patching [NCS18], [Ver19]. Notwithstanding, the overall hacking activity in the United Kingdom (UK) has fallen since 2018 [Cro19], [Pop+19b].

"Attacks on privacy and personal data" may lead to theft, manipulation, loss, or disclosure of data (e.g., credentials, financial information, names, social security numbers, birth dates) about individuals acting, inter alia, as organization's employees, customers, and suppliers [ICO18], [NCS18], [Ver19]. These attacks can be carried out through different techniques (e.g., phishing, spear-phishing, exploiting vulnerabilities, use of backdoor) and may cause financial distress and reputational harm to organizations if materialized [Acc18], [ENI19a], [GSM19], [NCS18], [Ver19]. Moreover, according to ENISA (2019a) [ENI19a], identity theft remains one of the most popular type of data breaches [Pop+19b].

"Cryptojacking" or cryptomining refers to an infection with a malware that runs surreptitiously on the victim's devices and enables the unauthorized use of the victim's computing power to mine cryptocurrencies (i.e., solving cryptographic puzzles to add transactions to the blockchain), and in turn, generate revenue for the attackers [Acc18], [ENI19a], [Ora19], [Sym19]. Hence, throughout 2017, there has been a shift among cyber criminals towards capitalizing on cryptomining malware, which prompted an increase in the cryptojacking activity [Acc18], [ENI19a], [NCS18]. Today, despite a major fall in cryptojacking events, cyber criminals still display significant interest in this way of generating money due to low entry barriers and minimal law enforcement attention [ENI19a], [Eur18], [Sym19], [Pop+19b].

"Cyber espionage" may come in two forms including state-sponsored cyber espionage and industrial espionage [Acc18], [Tha18]. The state-sponsored cyber espionage is led by cyber-espionage groups (e.g., MuddyWater, PIPEFISH aka OilRig, APT28, APT29) [Acc18], [Sym19]. These cyber espionage groups are doing malicious activities and developing malicious tools that may belong to one or more campaigns for exfiltrating trade or state secrets [Acc18], [ENI19a]. Throughout the campaigns, the cyber espionage groups are changing the techniques of their attacks [Acc18]. With respect to the industrial espionage, organizations are targeted by competitors aiming to gain commercial edge [Tha18]. As part of cyber espionage, hostile actors are incessantly leveraging the vulnerabilities introduced by the emerging technologies (e.g., IoT, Artificial Intelligence) [Acc18], [Boo19], [ENI19a]. Today, cyber espionage is among the greatest cyber threats to organizations [EY18b], [Tha18], [Pop+19b].

"Targeted attacks on critical infrastructure" target entities from critical sectors (e.g., energy, telecommunications, water utilities) that provide essential services for vital societal functions, health, safety, security, economic or social well-being of citizens, or the effective functioning of governments, and aim to sabotage their physical or virtual systems and assets [Pop+19a]. In this context, these are disruptive attacks that can inflict significant harm on a nation including, among others, compromise of national security or public safety, operational shutdowns, critical infrastructure breakdowns, substantial financial losses, or casualties [Acc18], [Sym19], [Tre18]. Moreover, there is limited information available about the activity associated with these types of cyberattacks given that most of the investigations fall within the remit of national security agencies [Eur18]. However, there is consensus that cyberattacks on critical infrastructure are becoming more and more prevalent considering, inter alia, the rise of Industrial Internet of Things (IIoT), the rates of convergence of information technology and operational technology, and the growing motivation of adversarial states to engage in and sponsor cyberattacks on critical infrastructures [Acc18], [Boo19], [Eur18], [WEF19], [Pop+19b].

"Supply chain attacks" are island hopping cyberattacks that rely on trusted and insecure third or fourth-party environments for the furtherance of malicious activity towards an end target [Acc18], [ENI18a], [NCS18], [Sym19]. These cyberattacks may take many forms including, among others, introducing exploitable vulnerabilities into third-party products or services, embedding malicious code into trusted third-party software, hijacking legitimate software updates, or infiltrating and harming target networks via third-party connections [Acc18], [NCS18], [Sym19]. Thus, nowadays, cyberattacks through trusted channels are increasingly attractive to cyber criminals [Acc18], [GSM19], [Sym19]. Also, according to Thales (2018) [Tha18] these attacks are among the greatest data security threats [Pop+19b].

"Cyberpropaganda" (aka information operations and warfare or influence operations) aims to advance economic, political, or military agendas through hybrid campaigns that blend a wide range of techniques encompassing, inter alia, propaganda operations, proliferation of disinformation, weaponized deepfakes, trolling, and espionage [Boo19], [NCS18], [Sym19]. Thus, these influence operations are driven by adversaries motivated to gain competitive advantage over their targets through Machiavellian means, and rely on unregulated dissemination channels (e.g., social media) to inflict significant disruption and destruction on their intended targets including reputational damage, share value depreciation, political instability, social unrest, and international conflicts, among others [Boo19], [NCS18], [Tre18]. Currently, cyberpropaganda remains a prominent cyber threat considering the difficulty associated with tackling the triad that enables disinformation spread (i.e., motivation, platforms, and tools) [Tre18], [Pop+19b].

"Legal and regulatory sanctions" represent a threat for organizations considering the ever-changing cybersecurity regulatory landscape (e.g., "EU General Data Protection Regulation", "Directive on Security of Network and Information Systems"), the stringent legal requirements coupled with the convergence and/or divergence between these legal requirements pertaining to the cybersecurity-related legislation within one or multiple jurisdictions where organizations operate [GSM19], [NCS18], [Pop+19a]. Moreover, non-compliance with applicable legislation might leave organizations susceptible to cyber-attacks, punitive sanctions, costly lawsuits following law infringements, and extortion payments to hostile actors [Acc18], [Tre18], [Pop+19a], [Pop+19b].

Hence, this catalogue of thirteen current cyber threat categories aims to serve as a starting point for organizations conducting cybersecurity risk assessments. However, considering that this catalogue of current cyber threat categories is not organization specific, organizations still need to engage in cyber threat profiling to form a thorough understanding of their cyber threat landscape. In this context, organizations need to rely on the existing cyber threat rating methods characterized by high complexity or uncertainty as they focus on the likelihood of threat initiation [NIS12a] or on the likelihood of a successful attack [OWA19]. Therefore, there is a need for a cyber threat rating method that is dissociated from the elements (e.g., skill level, motive, opportunity) that induce uncertainty and fosters unbiased outputs in a more consistent manner by focusing on the threat strength component of the cyber threat categories. Thus, Chapter 3 extends this research work on cyber threats by proposing a cyber threat rating method which provides a means to prioritize cyber threats, and by critically evaluating the thirteen cyber threat categories.

2.2. Overview of Cybersecurity Regulatory Landscape

Given the plethora of cybersecurity-related legislations and regulations from across the world [Giu+21], based on the information disseminated by the author through the research paper [Pop+19a], this subchapter provides an overview of the cybersecurity regulatory landscape that follows a laser-focused approach by targeting key cybersecurity-related legislations and regulations from key cybersecurity jurisdictions, and it aims to set the scene for establishing the degree of commonality between these legislations "from the perspective of the organizational understanding to managing cybersecurity risk" [Pop+19a]. In this context, this subchapter aims to exclusively focus on the jurisdictions that exhibit the highest levels of commitment towards cybersecurity across the globe considering that the cybersecurity-related legislations from the more mature cybersecurity jurisdictions are expected to have the greatest influence on the cybersecurity risk management practices of the organizations that operate in these jurisdictions [Pop+19a]. Moreover, this subchapter aims to concentrate on the cybersecurity-related areas of statute that are the most relevant for triggering the improvement of cybersecurity risk management practices in organizations [Pop+19a]. Thus, based on the information disseminated by the author through the research paper [Pop+19a], this subchapter provides an overview of some of the key generally applicable cybersecurity-related legislations and regulations pertaining to selected areas of statute under selected jurisdictions, and only addresses the statutes that were in force at the time of conducting the study on cybersecurity-related legislations.

First, for the selection of the in-scope jurisdictions, this subchapter relies upon the findings from the "Global Cybersecurity Index (GCI)" report which provides a benchmark measure to compare the level of commitment of countries towards cybersecurity on a global scale [ITU17]. In this context, at regional level, "GCI" ranks European Union (EU) as having the highest level of cybersecurity commitment worldwide based on the regional scorecard, while, at country level, the highest commitment towards cybersecurity worldwide resulted for Singapore and United States (US) respectively. Thus, based on the information disseminated by the author through the research paper [Pop+19a], the scope of this subchapter consists of and is limited to the following three jurisdictions, namely the EU, US, and Singapore [Pop+19a].

Then, this subchapter concentrates on some of the key legislations and regulations within the selected jurisdictions focused on "protecting the confidentiality, integrity, and availability (i.e., the CIA triad) of information and information systems and controlling access to information in the cyberspace [Kos18a], [Giu+21]" [Pop+19a]. Thus, two areas of statute are selected to be addressed under each of the in-scope jurisdictions, namely data protection and privacy area and critical infrastructure protection area, considering that these areas are directly steering organizations to enhance their cybersecurity maturity stance by fostering sound cybersecurity practices [Giu+21]. Therefore, the legislations under data protection and privacy area refer to the statutes prescribing data protection and privacy legal obligations on organizations which are using, storing, or transferring personal data in or outside their jurisdiction. In addition, the statutes under critical infrastructure protection area represent the cybersecurity laws prescribing requirements to prepare for, protect against, mitigate, respond to and recover from critical infrastructure disruptions, destruction or damage, where critical infrastructure means the physical or virtual systems and assets which are providing services essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of citizens or the effective functioning of governments within each jurisdiction [Com05], [Off08], [US01], [Off16c], [Aus17], [Pop+19a].

Despite that some of the laws may be classified across many areas, this subchapter links each law to the most relevant area. In addition, the subchapter is not targeting statutes applicable to specific cybersecurity products or services, the sector specific legislations and regulations related to cybersecurity, or the proposed laws and regulations which were not enacted at the time of conducting the study on the cybersecurity-related legislations. Also, this overview is not covering legislations and regulations pertaining to other cybersecurity-related areas of statute (e.g., export control, cybercrime). Moreover, with respect to the European Union (EU) and United States (US) jurisdictions, this overview is not focused on the laws applicable to specific EU Member States, or the ones related to specific US's Member States. Therefore, based on the information disseminated by the author through the research paper [Pop+19a], the categories of legislations and regulations pertaining to cybersecurity that are considered beyond the scope of this overview are listed below along with a few notable examples of enacted or proposed statutes [Pop+19a]:

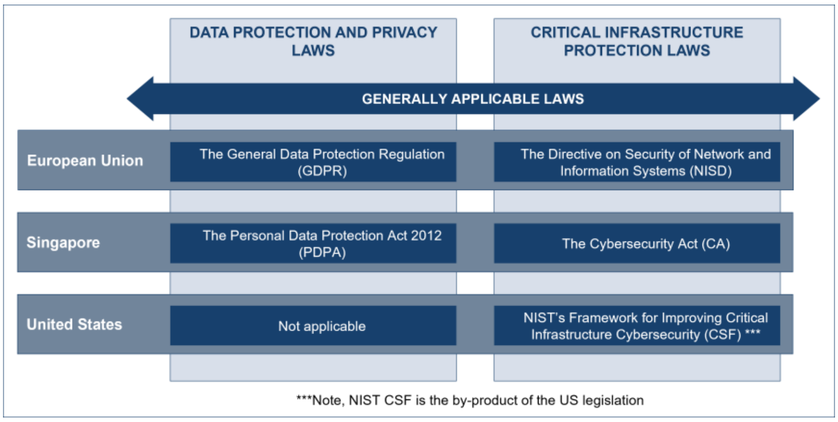
- "Legislations and regulations related to individual cybersecurity products or services", such as [Glo17]:
  - "European Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (i.e., eIDAS regulation)" [Pop+19a]
- "Sector specific legislations and regulations related to cybersecurity", such as [Giu+21], [Glo17], [Joh+14], [Law17]:
  - "the European Directive 2015/2366 (i.e., Payment Service Directive 2 – PSD2), the US Gramm-Leach-Bliley Act (GLBA), New York's Department of Financial Services Cybersecurity Regulation (NYFSC) for financial sector" [Pop+19a]
  - "European ePrivacy Directive applicable to electronic communications" [Pop+19a]
  - "the US Health Insurance Portability and Accountability Act (HIPAA) for health sector" [Pop+19a]
  - "the European Directive on data protection in law enforcement (i.e., Directive EU 2016/680) [Off16b], [Eur19]" [Pop+19a]
- "Legislations and regulations related to other cybersecurity-related areas of statute", such as:
  - "the European Council Regulation (EC) No 428/2009, the US Export Administration Regulations (EAR), the US Export Controls Act of 2018 (ECA), Singapore's Strategic Goods (Control) Act (Cap. 300) for the export control area [Off09], [Fer+18], [Glo17], [Gov03]" [Pop+19a]
  - "the European Directive on attacks against information systems (Directive 2013/40/EU), the US Computer Fraud and Abuse Act (CFAA), the US Electronic Communications Privacy Act (ECPA), the Singapore's Computer Misuse and Cybersecurity Act (CMCA) for the cybercrime area [Off13], [Doy14], [Kos18b], [Glo17], [Gov07]" [Pop+19a]
- "Proposed laws and regulations which were not enacted at the time of conducting the study on the cybersecurity-related legislations", such as:
  - "EU Cybersecurity Act [Cou17]" [Pop+19a]
  - "The US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) [US19]" [Pop+19a]
- "Statutes applicable to specific EU Member States / US's Member States" [Glo17]
- "International cooperation agreements", such as:
  - "EU-US Privacy Shield [Law17]" [Pop+19a]
  - "Budapest Convention on Cybercrime [Car16a]" [Pop+19a]

Furthermore, the existing research studies have different scope than the one of this study. In this context, some of the current literature has described the legal systems from one of the selected jurisdictions, namely the European Union (2018a)

[Eur18a], Carrapico and Barrinha (2017) [Car+17] and Johnson et al. (2014) [Joh+14] described the EU legal system; the Global Legal Group (2017) [Glo17] summarized the Singapore's legal system; and Fischer (2014) [Fis14], Pernik et al. (2016) [Per+16] and Global Legal Group (2017) [Glo17] outlined the US legal system [Pop+19a]. Moreover, other research works explored the statutes in silos (e.g., [Joh+14], [Cob+18], [Sir+18], [Eur18b], [ICO18], [Cro18]), provided an overview of the statutes from one jurisdiction (e.g., [Fir+17], [Kos18b]), or looked at areas of law in silos covering multiple jurisdictions (e.g., [DLA18]). In addition, some research works addressed laws covering multiple areas from multiple jurisdictions (e.g., [Glo17], [Häg+17], [Joh+14], [Rav+18], [Hog18], [Law17], [Sun+18]) without aiming to further explore the degree of commonality between these laws [Pop+19a].

It is worth noting that although there are numerous research studies that investigated cybersecurity-related legislations, no research work has been found that explores cybersecurity-related legislations for selected areas of statute from selected jurisdictions to establish the degree of commonality between them in the context of the organizational understanding to managing cybersecurity risk [Pop+19a]. Thus, to address the need of organizations operating in multiple jurisdictions to adopt a pragmatic approach towards achieving cybersecurity regulatory compliance [Pop+19a], the overview of the cybersecurity-related legislations from this chapter offers the starting point for the critical evaluation of these legislations, which is provided in Chapter 3.

Hence, based on the information disseminated by the author through the research paper [Pop+19a], the overview of legislations for the selected jurisdictions (i.e., European Union, Singapore, and United States) is provided below under individual sub-subchapters covering the selected areas of legislation (i.e., "data protection and privacy", "critical infrastructure protection") and using the the law libraries of the EU, Singapore, and US. Fig. 2.2 illustrates the selected cybersecurity legislation and regulation for each of the in-scope jurisdictions [Pop20].



	DATA PROTECTION AND PRIVACY LAWS	CRITICAL INFRASTRUCTURE PROTECTION LAWS
European Union	The General Data Protection Regulation (GDPR)	The Directive on Security of Network and Information Systems (NISD)
Singapore	The Personal Data Protection Act 2012 (PDPA)	The Cybersecurity Act (CA)
United States	Not applicable	NIST's Framework for Improving Critical Infrastructure Cybersecurity (CSF) ***

***Note, NIST CSF is the by-product of the US legislation

Fig. 2.2. Selected cybersecurity legislations [Pop20]

2.2.1. Cybersecurity Legislation and Regulation in the European Union

Cybersecurity has been one of the main security priorities for the EU to enable the creation of an open, safe, and secure cyberspace as proposed within the "EU 2013 Cybersecurity Strategy", which has also been reflected by the enactment of many EU cybersecurity legislations and regulations [Car+17], [Car+18], [Joh+14]. In this context, the EU legal framework comprises several types of legal acts of which some are legally binding while others are not and apply either to all 27 EU Member States or to just a few entities [Eur18a]. Thus, based on the information disseminated by the author through the research paper [Pop+19a], this sub-subchapter provides an overview of some of the key EU cybersecurity laws by addressing the statutes relevant to each of the selected areas outlined above [Pop+19a].

With respect to data protection and privacy obligations, at EU level "the General Data Protection Regulation (EU) 2016/679 (GDPR)" brings stringent data protection and privacy requirements applicable globally to organizations processing and controlling personal data of EU and European Economic Area (EEA) citizens, and guarantees, inter alia, data protection rights of the data subject (e.g., "right of access", "rectification", "erasure", "restriction", "objection", and "data portability") [Off16a], [Cob+18], [Eur18b], [Giu+21], [Pop+19a].

As for the critical infrastructure protection area, EU has "the Directive on Security of Network and Information Systems (NISD)" which binds all EU Member States, and mandates the achievement of "a high common level of security of network and information systems across EU" through measures related to the development of national frameworks on the security of network and information systems by each EU Member State, measures concerning the strategic cooperation between EU Member States, and risk management and incident reporting obligations to operators of critical infrastructure identified by each EU Member State (i.e., "the Operators of Essential Services – OESs" and "the Digital Service Providers – DSPs") [Off16c], [Giu+21], [Pop+19a].

2.2.2. Cybersecurity Legislation and Regulation in Singapore

Singapore has established a comprehensive cybersecurity legislation framework including many recent and fast-paced legislative developments [Hog18], [Law17]. The resulting cybersecurity-related requirements are pursuant to "Singapore's National Cybercrime Action Plan", namely the strengthening of cybercrime laws, and as set forth in the "Singapore's Cybersecurity Strategy" aiming towards a more resilient and trusted cyberspace for Singaporeans to harness the benefits of technology by "countering cyber threats, combating cybercrime, and protecting personal data [Gov16], [Sin16]" [Pop+19a]. Furthermore, these requirements are either general or sectoral in their application [Glo17]. Therefore, based on the information disseminated by the author through the research paper [Pop+19a], this sub-subchapter outlines some of the main cybersecurity-related laws that are generally applicable across Singapore under the selected areas [Pop+19a].

First, in terms of data protection and privacy, "the Personal Data Protection Act 2012 (PDPA)" provides requirements governing the collection, use and disclosure of personal data from individuals in Singapore by private organizations irrespective of whether their geographic operations or incorporation are in or outside of Singapore, or, in other words, the requirements have extraterritorial effect [DLA18], [Gov12], [PDP17], [Sun+18]. Additionally, the "PDPA" established "the Personal Data Protection Commission (PDPC)" with the main responsibility of conducting oversight and enforcement of the "PDPA" [DLA18], [Glo17], [Law17], [PDP17], [Pop+19a].

With respect to critical infrastructure protection, Singapore enacted "the Cybersecurity Act (CA)" that aims to enhance "the Critical Information Infrastructure (CII)" against cyber threats by establishing a legal framework with cybersecurity-related requirements imposed on owners of "CII" located either wholly or partially in Singapore [Glo17], [Gov18]. Hence, among others, the "CA" prescribes requirements for the licensing of providers of relevant cybersecurity services, and the appointment of a Commissioner of Cybersecurity (i.e., the Commissioner) for the designation of "CII" and the enforcement of the provisions of the "CA", just to name a few of the responsibilities [Gov18], [Pop+19a].

2.2.3. Cybersecurity Legislation and Regulation in the United States

In the US, over 50 statutes feed into the framework legislation regarding cybersecurity [Fis14], [Per+16]. The legal framework in question takes the shape of a matrix of federal and state laws, regulations and private industry requirements applying either horizontally (i.e., spanning across sectors) or vertically (i.e., sector-specific) [Glo17], [US17]. Thus, in order to highlight some of the key laws and regulations pertaining to cybersecurity that apply to all 50 states, the District of Columbia, and US territories, based on the information disseminated by the author through the research paper [Pop+19a], this sub-subchapter provides a brief overview of the US federal laws related to the selected areas [Pop+19a].

First, with respect to data protection and privacy area, despite its well-documented history of law [Hat+15], the US requirements are prescribed merely vertical (i.e., sectoral) rather than horizontal (i.e., general) in their application [Glo17], [Jol19], [Rav+18], [US17]. Furthermore, at the time of conducting the study on the cybersecurity-related legislations, there was no general law applicable to data protection and privacy at federal level in the US [Pop+19a].

The second area, namely the critical infrastructure protection, relates to "section 1016 (i.e., Critical Infrastructures Protection Act of 2001) of the PATRIOT Act" that defined the critical infrastructure and set forth the policy of the US to strengthen critical infrastructures through greater engagement in public-private partnerships [US01]. In addition, at federal level, "the Executive Order 13636 (i.e., Improving Critical Infrastructure Cybersecurity)", "the Presidential Policy Directive-21 (i.e., Critical Infrastructure Security and Resilience)", and "the Presidential Executive Order 13800 (i.e., Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)" called for greater situational awareness through enhanced collaboration and information sharing, a more holistic approach to cybersecurity, and the improvement of cybersecurity risk management capabilities and maturity posture including the making of a technology neutral voluntary cybersecurity framework, namely "the NIST's Framework for Improving Critical Infrastructure Cybersecurity (i.e., the NIST CSF)" [The13a], [The13b], [The17], [Pop+19a].

2.3. Overview of Cybersecurity Risk Management Frameworks

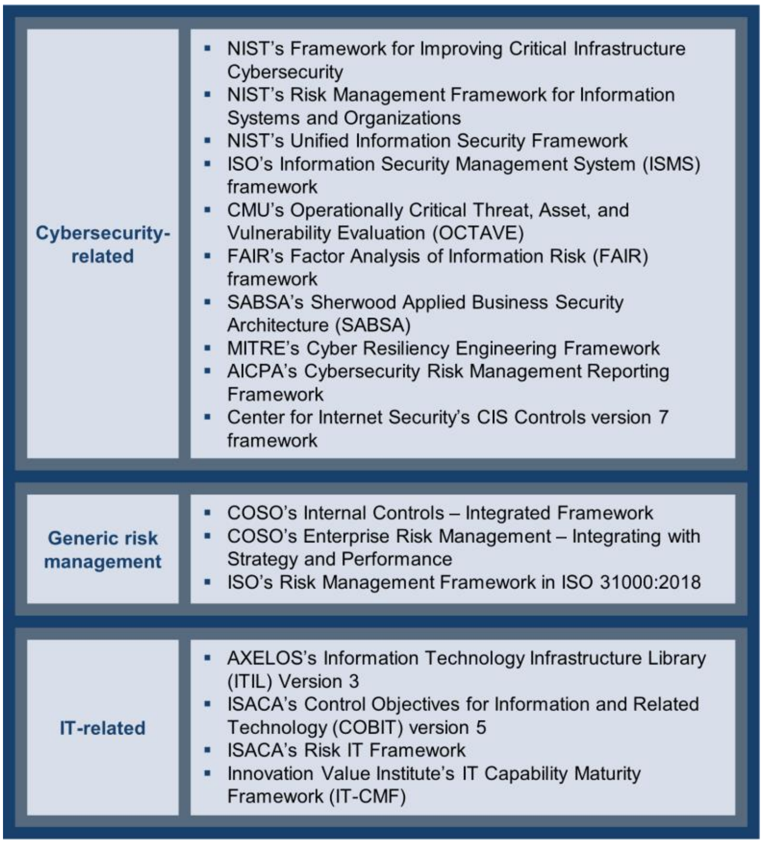
Based on the information disseminated by the author through the research paper [Giu+21], much of the research up to now has been focused on oulining cybersecurity and risk management related frameworks, standards, and methodologies without clearly delineating the distinction between them [Twe+18]. Other research works have provided overviews of frameworks pertaining to specific focus areas [Cur+16], [Inn10]. While oher works merely focused on risk management-related methodologies and standards. Thus, WISER Consortium (2016) [WIS16] outlined standards and methods for risk management, security testing and vulnerability and threat monitoring; ENISA (2006) [ENI06] provided an inventory of risk management / assessment methods; Ionita (2013) [Ion13] provided a survey of risk management / assessment methods; Talabis and Martin (2013) [Tal+13] provided a high-level overview of some information security risk assessment frameworks and of the information security risk management standard ISO 27005; the Department for Business, Innovation and Skills (2013) [Cro13] presented a high-level cybersecuity landscape including standards and frameworks / methodologies; and Taubenberger (2014) [Tau14] described the state of the art for information security risk management-related standards and methods.

Furthermore, based on the information disseminated by the author through the research paper [Giu+21], while "framework enablers (e.g., policies, standards, processes, procedures, methodologies, methods, tools, etc.) underpin the implementation of and allow frameworks to achieve their intended outcomes, specifically of effectively managing cybersecurity risks in accordance with organization's risk appetite", frameworks are "the nucleus of cybersecurity risk management programmes" [Giu+21]. Hence, based on the information disseminated by the author through the research paper [Giu+21], this subchapter provides an overview of several well-renowned cybersecurity risk management frameworks. "As the terms standards, frameworks, methods and methodologies are used interchangeably in the literature pertaining to the management of cybersecurity risks", this subchapter begins by defining the cybersecurity risk management frameworks followed by an overview of the most widely adopted frameworks [Giu+21]. Thus, based on the information disseminated by the author through the research paper [Giu+21], a cybersecurity risk management framework is "a structured overarching approach which relies on a set of guiding principles and sets the context within which cybersecurity risks can be consistently overseen and managed across an organization to support leadership oversight, integration, design, implementation, evaluation and continuous improvement initiatives of the cybersecurity risk management programme [Rog+16], [CNS15], [Axe12], [ISO18b], [IRM18], [ISO09], [ISO18c], [ENI06], [WIS16], [ISA09], [Gas+17], [Inn10], [ENI08]" [Giu+21]. Hence, based on the information disseminated by the author through the research paper [Giu+21], organizations are provided with "a logical structure or model which may not get into the detailed processes and procedures, supported by a collection of standards and best practices (e.g., methodologies, methods, etc.) to apply their underlying principles, build, and run cybersecurity risk management programmes, and in effect, effectively manage cybersecurity risks at all levels (i.e., the organizational, mission/business process, and information system levels) in accordance with the organization's objectives and overall risk strategy [Rog+16], [ISO18b], [WIS16], [Tal+13], [NIS13]" [Giu+21].

Based on the information disseminated by the author through the research paper [Giu+21], "there are numerous frameworks in the literature relevant to managing cybersecurity risks, which can be leveraged by organizations, and each framework provides specific guidance and best practice applicable to one or more domains [ENI06], [WIS16], [Cro13], [Tau14], [Ion13]" [Giu+21]. Therefore, "although this overview does not provide an exhaustive list of frameworks", it offers an overview of several widely used frameworks pertaining to three categories relevant for cybersecurity risk management "which can be leveraged by any organization regardless of type, size, sector, or focus area (e.g., Information Technology (IT), Industrial Control Systems (ICS), Cyber-Physical Systems (CPS), or connected devices)", including [Giu+21]:

- "Cybersecurity-related frameworks";
- "Generic risk management frameworks";
- "IT-related frameworks".

Further, Fig. 2.3 outlines the selected frameworks pertaining to the aforementioned categories relevant to cybersecurity risk management.



Cybersecurity-related	▪ NIST's Framework for Improving Critical Infrastructure Cybersecurity ▪ NIST's Risk Management Framework for Information Systems and Organizations ▪ NIST's Unified Information Security Framework ▪ ISO's Information Security Management System (ISMS) framework ▪ CMU's Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) ▪ FAIR's Factor Analysis of Information Risk (FAIR) framework ▪ SABSA's Sherwood Applied Business Security Architecture (SABSA) ▪ MITRE's Cyber Resiliency Engineering Framework ▪ AICPA's Cybersecurity Risk Management Reporting Framework ▪ Center for Internet Security's CIS Controls version 7 framework
Generic risk management	▪ COSO's Internal Controls – Integrated Framework ▪ COSO's Enterprise Risk Management – Integrating with Strategy and Performance ▪ ISO's Risk Management Framework in ISO 31000:2018
IT-related	▪ AXELOS's Information Technology Infrastructure Library (ITIL) Version 3 ▪ ISACA's Control Objectives for Information and Related Technology (COBIT) version 5 ▪ ISACA's Risk IT Framework ▪ Innovation Value Institute's IT Capability Maturity Framework (IT-CMF)

Fig. 2.3. Selected cybersecurity risk management frameworks [Pop20]

Consequently, based on the information disseminated by the author through the research paper [Giu+21], the tables below (i.e., Tables 2.1, 2.2, and 2.3) provide an overview of the most widely adopted frameworks relevant to cybersecurity risk management by mapping each framework to its corresponding category (i.e., "cybersecurity", "risk management", "IT"), and outline for each framework the following details: "publisher name", "short description", and "access (i.e., free of charge, not freely available, freely available to members)" [Giu+21].

Firstly, based on the information disseminated by the author through the research paper [Giu+21], Table 2.1 provides an overview of the most widely adopted cybersecurity-related frameworks [Giu+21]. Many frameworks pay particular attention to cybersecurity, and this is reflected by "the large number of existing frameworks relevant to the cybersecurity-related domain" (see Table 2.1) [Giu+21]. As shown in Table 2.1, the cybersecurity-related frameworks are applicable to either "risk assessment" or "risk management" activities [Ion13] and are supported by a "risk-based" [ENI06], [Gas+17], [Tal+13] or "compliance-based" approach (i.e., aka "rule-based") [Rog+16], [Ion13], [Giu+21].

Table 2.1. Overview of selected cybersecurity-related frameworks [Giu+21]

Framework Name	Publisher	Description	Access
"Framework for Improving Critical Infrastructure Cybersecurity"	"National Institute of Standards and Technology (NIST)"	"Provides a common language for identifying and managing cybersecurity risks and consists of three components: Framework Core (i.e., a common set of activities and references to be used as guidance), Framework Implementation Tiers (i.e., a range of Tiers from Partial to Adaptive to support organizational decision making) and Framework Profiles (i.e., to describe current or target organizational profiles of specific cybersecurity activities) [NIS18a]. It can be applied by any organization regardless of sector, size, or type, even if the framework was developed to improve cybersecurity risk management in critical infrastructure [NIS18a]" [Giu+21].	Free of charge
"Risk Management Framework (RMF) for Information Systems and Organizations"	"National Institute of Standards and Technology (NIST)"	"Provides a structured and flexible process to effectively manage information security risks from organizational level to system level, and consists of seven main activities (i.e., prepare, categorize, select, implement, assess, authorize, and monitor) with detailed description for each of the tasks involved in each activity; RMF is intended to support the implementation of the NIST's cybersecurity framework [NIS10]" [Giu+21].	Free of charge
"NIST's Unified Information Security Framework"	"National Institute of Standards and Technology (NIST)"	"Consists of five Special Publications (SPs) from NIST, such as: NIST SP 800-37 (i.e., RMF) [NIS10], NIST SP 800-53 (i.e., recommended security and privacy controls) [NIS13], NIST 800-53A (i.e., guide for assessing the security and privacy controls) [NIS14], NIST SP 800-30	Free of charge

Framework Name	Publisher	Description	Access
		(i.e., guide for conducting risk assessments) [NIS12a] and NIST SP 800-39 (i.e., guidance for organization-wide program for managing information security risks) [NIS11]" [Giu+21].	
"Information Security Management System (ISMS) framework"	"International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)"	"Provides policies, procedures, and resources to allow a systematic approach for establishing, implementing, monitoring, reviewing, maintaining, and improving an ISMS in accordance with the needs and objectives of the organization across different operations and sites. It is based on the ISMS family of standards, which consists of: standards specifying requirements (i.e., ISO/IEC 27001, ISO/IEC 27006, ISO/IEC 27009), standards specifying guidelines (i.e., ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, ISO/IEC TR 27008, ISO/IEC 27013, ISO/IEC 27014, ISO/IEC TR 27016, ISO/IEC 27021), and standards describing sector specific guidelines (i.e., ISO/IEC 27010, ISO/IEC 27011, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27019) [ISO18b], [ENI06], [WIS16], [Tau14]" [Giu+21].	Not freely available
"Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)"	"Software Engineering Institute (SEI) of Carnegie Mellon University (USA)"	"It is an information security risk assessment framework which consists of a collection of tools, techniques, and methods, having three different versions: OCTAVE (i.e., the original framework which is recommended for large organizations and resembles a methodology), OCTAVE-S (i.e., developed for smaller organizations) and OCTAVE Allegro (i.e., the most recent version of the framework) [WIS16], [Tal+13], [Ion13], [SEI07]" [Giu+21].	Free of charge
"Factor Analysis of Information Risk (FAIR) framework"	"FAIR Institute"	"It is a logical framework for conducting information risk assessments, which consists of the following elements: the taxonomy of information risks and of their risk factors (i.e., probable frequency and probable magnitude of future loss), a method for computing the risk factors, a computational engine for estimating risks along with a simulation model to build and analyze risk scenarios [Ion13], [Jon06], [Twe+18], [Ful17]" [Giu+21].	Free of charge
"Sherwood Applied Business Security	"SABSA Institute"	"It is an Enterprise Security Architecture framework and consists of six architecture layers (i.e., contextual, conceptual, logical, physical, component and management architectures) which are presented through	Free of charge

Framework Name	Publisher	Description	Access
Architecture (SABSA)"		SABSA Matrix where these layers are mapped to the phases of the SABSA's risk management process (i.e., assure, strategy and planning, design, implement, manage and measure, communicate). Beside the SABSA Matrix, the framework provides the SABSA Business Attributes Profile which highlights what organizations need to protect [She+09], [Van14]" [Giu+21].	
"Cyber Resiliency Engineering Framework"	"The MITRE Corporation"	"Provides elements related to cyber resiliency (i.e., goals, objectives, practices), threat modelling, domains for applying cyber resiliency, along with costs considerations [Bod+11]" [Giu+21].	Free of charge
"Cybersecurity Risk Management Reporting Framework"	"The American Institute of Certified Public Accountants (AICPA)"	"Consists of three components: description criteria for management's description of the entity's cybersecurity risk management program, control criteria for evaluating the effectiveness of the security controls, along with AICPA's attestation guide reporting on an entity's cybersecurity risk management program and controls [AIC17a]" [Giu+21].	Free of charge
"CIS Controls version 7 framework"	"Center for Internet Security (CIS)"	"Provides 20 security controls which are split in three categories (i.e., basic, foundational, and organizational) to assist organizations with a defense-in-depth set of best practices [CIS18c]" [Giu+21].	Free of charge

Secondly, based on the information disseminated by the author through the research paper [Giu+21], Table 2.2 shows an overview of the most adopted "generic risk management frameworks", which provide "generic control objectives", "internal controls", "principles", or "guidelines on risk management" [IRM18], [WIS16], [ISA09], [Ion13], [COS13], [COS17], [Giu+21].

Table 2.2. Overview of selected generic risk management frameworks [Giu+21]

Framework Name	Publisher	Description	Access
"COSO's Internal Controls – Integrated Framework"	"Committee of Sponsoring Organizations of the Treadway Commission (COSO)"	"Encompasses the following elements: three objectives (i.e., operations, reporting, and compliance), five components of internal controls (i.e., control environment, risk assessment, control activities, information and communication, and monitoring activities) and seventeen principles. It is valuable for designing, implementing, assessing, and reporting internal controls to reduce and manage risks across organizations [COS13], [COS17]" [Giu+21].	Not freely available

Framework Name	Publisher	Description	Access
"COSO's Enterprise Risk Management – Integrating with Strategy and Performance"	"Committee of Sponsoring Organizations of the Treadway Commission (COSO)"	"Provides five components (i.e., governance and culture; strategy and objective-setting; performance; review and revision; information, communication, and reporting), which are supported by a set of principles, for identifying and managing enterprise-wide risks associated with the organization's strategy and business objectives, and for sustaining and improving performance [COS17]" [Giu+21].	Not freely available
"Risk Management Framework in ISO 31000:2018"	"International Organization for Standardization (ISO)"	"Provides guidelines about the range of activities involved in a risk management initiative, and describes six elements: leadership and commitment, integration, design, implementation, evaluation, and improvement [IRM18], [ISO18d]" [Giu+21].	Not freely available

Further, based on the information disseminated by the author through the research paper [Giu+21], Table 2.3 indicates an overview of the most widely adopted "IT-related frameworks". These frameworks are "neither cybersecurity-centric nor generic risk management frameworks and are largely focused on IT and belong to the following focus areas: IT service management, enterprise IT governance and management, enterprise-wide IT risk management, or IT capability management" [Rog+16], [Giu+21].

Table 2.3. Overview of selected IT-related frameworks [Giu+21]

Framework Name	Publisher	Description	Access
"Information Technology Infrastructure Library (ITIL) Version 3"	"Axelos"	"It is an IT service management framework having five core publications (i.e., service strategy, service design, service transition, service operation, and continual service improvement) which contain 26 processes, to facilitate the delivery and management of high-quality IT services [Dav16]" [Giu+21].	Not freely available
"Control Objectives for Information and Related Technology (COBIT) version 5"	"Information Systems Audit and Control Association (ISACA) - IT Governance Institute (ITGI)"	"It is an enterprise IT governance and management framework that belongs to the COBIT 5 product family and is built on five basic principles (i.e., meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, enabling a holistic approach, and separating governance from management) [ISA12]. It consists of high-level controls objectives and controls for IT, grouped into four domains: plan and organize, acquire and implement, deliver and support, and monitor and evaluate [Tau14]" [Giu+21].	Not freely available

Framework Name	Publisher	Description	Access
“Risk IT Framework”	“Information Systems Audit and Control Association (ISACA)”	“Provides an end-to-end process model with three domains (i.e., risk governance, risk evaluation, and risk response) for effective management of IT risk, which is based on several guiding principles and good practice guidance [ISA09]” [Giu+21].	Not freely available
“IT Capability Maturity Framework (IT-CMF)”	“Innovation Value Institute™”	“Consists of four macro-capabilities (i.e., managing IT like a business, managing the IT budget, managing the IT capability, and managing IT for business value) which are provided with their corresponding critical capabilities. For each critical capability, IT-CMF incorporates a comprehensive suite of capability building blocks, maturity profiles, assessment methods, and improvement roadmaps [Cur+16]” [Giu+21].	Not freely available

Thus, given the myriad of cybersecurity risk management frameworks, there is a need for more evaluations of these frameworks relative to each other to enable better decision making when it comes to framework selection, considering that these frameworks are the nucleus of cybersecurity risk management programmes in organizations [Giu+21], and taking into account the paucity of research works that provide a comprehensive characterization of several of these frameworks relative to each other [Giu+21]. Hence, building on this overview of cybersecurity risk management frameworks, Chapter 4 proposes a framework evaluation methodology and critically evaluates some of these frameworks.

2.4. Overview of IoT Security Best Practices

Based on the information disseminated by the author through the research paper [Pop+21a], “there are numerous best practices in the literature relevant to IoT security” [Pop+21a]. 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” [Pop+21a]. In this context, the identification of the in-scope IoT security best practices is based on “the current state of the art” (i.e., [ECS17], [Gar+19]), “available mappings of IoT security recommendations, guidance and standards to IoT security best practices” (i.e., [Cop20], [CSD19], [DCM18b], [ENI17b], [NIS20b]), and “references to IoT security best practices from other research works” (i.e., [ETS20], [W3C19]) [Pop+21a]. This identification of IoT security best practices 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)” [Pop+21a]. 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” [Pop+21a]. Moreover, this overview focuses on “final versions of IoT security best practices and does not cover draft or expired ones” [Pop+21a]. 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" [Pop+21a]. Therefore, based on the information disseminated by the author through the research paper [Pop+21a], 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 [Pop+21a]:

- "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) [IET17]" [Pop+21a]
- "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 [CTI21]" [Pop+21a]
  - "PSA Certified™ Level 1 Questionnaire, Version 2.1 published by Platform Security Architecture (PSA) Joint Stakeholder Agreement (JSA) Members [PSA21]" [Pop+21a]
- "Draft IoT security best practices", such as:
  - "oneM2M TR-0008-V2.0.1 Security (Technical Report) issued by oneM2M Partners [one18]" [Pop+21a]
- "Expired IoT security best practices", such as:
  - "Best Current Practices for Securing Internet of Things (IoT) Devices [Moo+17]" [Pop+21a]
- "Cybersecurity best practices that are not IoT security specific", such as:
  - "The Open Web Application Security Project (OWASP) Secure Coding Practices Quick Reference Guide [OWA10]" [Pop+21a]
  - "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) [Bel+11]" [Pop+21a]
  - "Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure System published by National Institute of Standards and Technology (NIST) [Ros+16]" [Pop+21a]
- "Vendor reports covering IoT security best practices", such as:
  - "AT&T Cybersecurity Insights: The CEO's Guide to Securing the Internet of Things [AT&T16]" [Pop+21a]

Thus, based on the information disseminated by the author through the research paper [Pop+21a], Table 2.4 illustrates the 25 selected IoT security best practices, and outlines for each best practice its corresponding "publisher" and "reference" [Pop+21a].

Table 2.4. Selected IoT security best practices [Pop+21a]

Publisher	Name	Reference
"AgeLight LLC"	"IoT Safety Architecture & Risk Toolkit v4.0"	[Age20a]
"Alliance for Internet of Things Innovation (AIOTI)"	"Report on Workshop on Security and Privacy in the Hyper-Connected World"	[AIO16]
"Australian Government"	"Code of Practice Securing the Internet of Things for Consumers"	[Com20]

Publisher	Name	Reference
"Broadband Internet Technical Advisory Group (BITAG)"	"Internet of Things (IoT) Security and Privacy Recommendations"	[BIT16]
"Cloud Security Alliance (CSA)"	"Security Guidance for Early Adopters of the Internet of Things (IoT)"	[CSA15]
"Cloud Security Alliance (CSA)"	"Identity and Access Management for the Internet of Things - Summary Guidance"	[CSA16]
"Cloud Security Alliance (CSA)"	"CSA IoT Security Controls Framework Version 1"	[CSA19a]
"Council to Secure the Digital Economy (CSDE)"	"The C2 Consensus on IoT Device Security Baseline Capabilities"	[CSD19]
"European Telecommunications Standards Institute (ETSI)"	"ETSI European Standard (EN) 303.645 V2.1.1 Cyber Security for Consumer Internet of Things: Baseline Requirements"	[ETS20]
"GSM Association (GSMA)"	"GSMA IoT Security Assessment Checklist Version 3.0"	[GSM18]
"Industrial Internet Consortium (IIC)"	"Industrial Internet of Things Volume G4: Security Framework"	[IIC16]
"Institute of Electrical and Electronics Engineers (IEEE)"	"Internet of Things (IoT) Security Best Practices"	[IEE17]
"IoT Security Foundation (IoTSF)"	"IoT Security Compliance Framework Release 2.1"	[IoT20a]
"Japan's IoT Acceleration Consortium (IoTAC)"	"IoT Security Guidelines Ver. 1.0"	[IoT16]
"National Electrical Manufacturers Association (NEMA)"	"Cyber Hygiene Best Practices"	[NEM18]
"National Institute of Standards and Technology (NIST)"	"Foundational Cybersecurity Activities for IoT Device Manufacturers"	[NIS20a]
"Online Trust Alliance (OTA)"	"IoT Security & Privacy Trust Framework v2.5"	[OTA18]
"The European Union Agency for Cybersecurity (ENISA)"	"Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures"	[ENI17b]
"The European Union Agency for Cybersecurity (ENISA)"	"Good Practices for Security of Internet of Things in the context of Smart Manufacturing"	[ENI18b]
"The European Union Agency for Cybersecurity (ENISA)"	"Good Practices for Security of IoT Secure Software Development Lifecycle"	[ENI19b]
"The European Union Agency for Cybersecurity (ENISA)"	"Procurement Guidelines for Cybersecurity in Hospitals Good practices for the security of Healthcare services"	[ENI20a]

Publisher	Name	Reference
"The European Union Agency for Cybersecurity (ENISA)"	"Guidelines for Securing the Internet of Things Secure supply chain for IoT"	[ENI20b]
"US Department of Homeland Security (DHS)"	"Strategic Principles for Securing the Internet of Things (IoT) Version 1.0"	[DHS16]
"US Department of Transportation National Highway Traffic Safety Administration (NHTSA)"	"Cybersecurity Best Practices for Modern Vehicles"	[NHT16]
"United Kingdom Department for Digital, Culture, Media and Sport (UK DCMS)"	"Code of Practice for Consumer IoT Security"	[DCM18a]

Furthermore, based on the information disseminated by the author through the research paper [Pop+21a], Fig. 2.4 illustrates the proposed taxonomic hierarchy for "classifying the 25 selected IoT security best practices, which emerged from the review of these IoT security best practices" [Pop+21a]. This 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" [Pop+21a]. Thus, based on the information disseminated by the author through the research paper [Pop+21a], 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" [Pop+21a];
- **"General"**: "this category denotes IoT security best practices that are applicable to IoT adopters, IoT manufacturers and/or IoT suppliers" [Pop+21a];
- **"Manufacturer specific"**: "this category denotes IoT security best practices that are applicable primarily to IoT manufacturers" [Pop+21a];
- **"Supplier specific"**: "this category denotes IoT security best practices that are applicable primarily to IoT suppliers" [Pop+21a].

As for the next level of the taxonomic hierarchy, based on the information disseminated by the author through the research paper [Pop+21a], 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 [Com20] or guidelines [DCM18a] recommended by governments for industry as the minimum standard for a specific topic [Com20], which do not take precedence over national legislation in any country [Fle+88]" [Pop+21a];
- **"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 [Giu+21]" [Pop+21a];
- **"Guidelines":** "this category denotes IoT security recommendations on how something should be done for achieving an objective [ENI13], and these recommendations are less prescriptive than procedures [ISA21]" [Pop+21a];

- **"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 [Giu+21]" [Pop+21a].

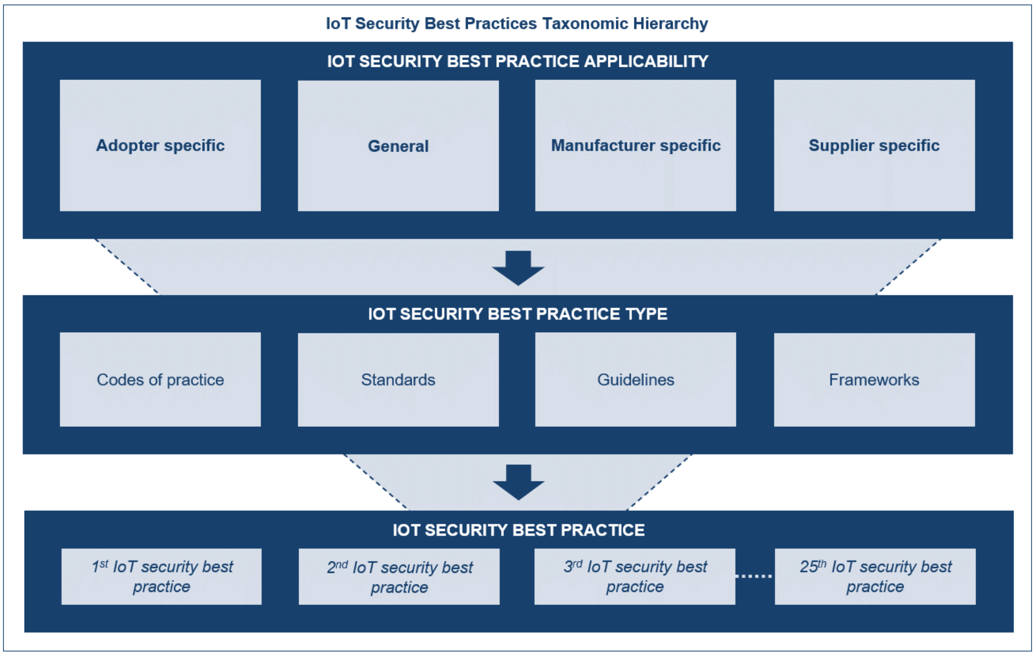

IoT Security Best Practices Taxonomic Hierarchy
IOT SECURITY BEST PRACTICE APPLICABILITY
Adopter specific
General
Manufacturer specific
Supplier specific
IOT SECURITY BEST PRACTICE TYPE
Codes of practice
Standards
Guidelines
Frameworks
IOT SECURITY BEST PRACTICE
1st IoT security best practice
2nd IoT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

Fig. 2.4. The proposed taxonomic hierarchy for IoT security best practices [Pop+21a]

Furthermore, based on the information disseminated by the author through the research paper [Pop+21a], some of the previous studies concentrated on "the state of the art of IoT security best practices (i.e., [ECS17], [Gar+19])" or on "delivering an overview and catalogue of key IoT security initiatives [CSA19c]" [Pop+21a]. For instance, ECSO (2017) [ECS17], Garcia-Morchon, et al. (2019) [Gar+19], and CSA Singapore along with MEAC of the Netherlands (2019c) [CSA19c] "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)" [Pop+21a]. Hence, besides providing an overview of some of the most renowned IoT security best practices, this subchapter proposes 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" [Pop+21a].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21a], Table 2.5 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 [Pop+21a].

Table 2.5. Selected IoT security best practices with their taxonomic categories [Pop+21a]

Applicability	Type	IoT Security Best Practice	Reference
"Adopter specific"	"Guidelines"	"CSA's Security Guidance for Early Adopters of the Internet of Things (IoT)"	[CSA15]
		"CSA's Identity and Access Management for the Internet of Things—Summary Guidance"	[CSA16]
		"ENISA's Procurement Guidelines for Cybersecurity in Hospitals Good practices for the security of Healthcare services"	[ENI20a]
	"Frameworks"	"CSA IoT Security Controls Framework Version 1"	[CSA19a]
"General"	"Codes of practice"	"US DHS's Strategic Principles for Securing the Internet of Things (IoT) Version 1.0"	[DHS16]
		"Japan's IoTAC IoT Security Guidelines Ver. 1.0"	[IoT16]
	"Guidelines"	"ENISA's Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures"	[ENI17b]
		"ENISA's Good Practices for Security of Internet of Things in the context of Smart Manufacturing"	[ENI18b]
		"ENISA's Good Practices for Security of IoT Secure Software Development Lifecycle"	[ENI19b]
		"ENISA's Guidelines for Securing the Internet of Things Secure supply chain for IoT"	[ENI20b]
	"Frameworks"	"AgeLight's IoT Safety Architecture & Risk Toolkit v4.0"	[Age20a]
		"IIC's Industrial Internet of Things Volume G4: Security Framework"	[IIC16]
		"OTA's IoT Security & Privacy Trust Framework v2.5"	[OTA18]
"Manufacturer specific"	"Standards"	"ETSI European Standard (EN) 303.645 V2.1.1 Cyber Security for Consumer Internet of Things: Baseline Requirements"	[ETS20]
		"NEMA's Cyber Hygiene Best Practices"	[NEM18]
	"Guidelines"	"BITAG's Internet of Things (IoT) Security and Privacy Recommendations"	[BIT16]
		"CSDE's The C2 Consensus on IoT Device Security Baseline Capabilities"	[CSD19]
		"IEEE's Internet of Things (IoT) Security Best Practices"	[IEE17]

Applicability	Type	IoT Security Best Practice	Reference
		“NIST’s Foundational Cybersecurity Activities for IoT Device Manufacturers”	[NIS20a]
“Supplier specific”	“Codes of practice”	“UK DCMS’s Code of Practice for Consumer IoT Security”	[DCM18a]
		“Australian Government’s Code of Practice Securing the Internet of Things for Consumers”	[Com20]
	“Guidelines”	“AIOTI’s Report on Workshop on Security and Privacy in the Hyper-Connected World”	[AIO16]
		“US NHTSA’s Cybersecurity Best Practices for Modern Vehicles”	[NHT16]
	“Frameworks”	“GSMA’s IoT Security Assessment Checklist Version 3.0”	[GSM18]
		“IoTSF’s IoT Security Compliance Framework Release 2.1”	[IoT20a]

It is worth noting that “although a sizeable number of best practices and academic papers has been published on IoT security”, “no research article nor best practice has been found at the time of conducting this study to exclusively focus on IoT security risk management strategy and there is a paucity of IoT security risk management reference sources” [Pop+21a]. In this context, there is a need for “a reference model for IoT security risk management strategy” [Pop+21a]. Thus, the overview of the IoT security best practices from this subchapter aims to support the development of the IoT security risk management strategy reference model which is provided in Chapter 5.

Furthermore, based on the information disseminated by the author through the research paper [Pop+21a], an overview of these IoT security best practices is provided under individual sub-subchapters that correspond to the four categories of IoT security best practices based on “their applicability to specific groups of target audience” [Pop+21a]. In addition, the available documentation around the 25 selected IoT security best practices is used to provide the overview of IoT security best practices [Pop+21a]. Then, as part of each sub-subchapter, the corresponding IoT security best practices are outlined under their corresponding category based on “the type of IoT security best practice” [Pop+21a].

2.4.1. Adopter Specific IoT Security Best Practices

Based on the information disseminated by the author through the research paper [Pop+21a], this sub-subchapter 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” [Pop+21a].

“Adopter Specific IoT Security Guidelines”

The IoT security best practices below are guidelines that address “generic-based IoT security controls [CSA15]”, “IoT recommendations specific to Identity and

Access Management [CSA16]", or "healthcare-specific IoT security good practices [ENI20a]" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a], 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 [Gar+19]. 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 [CSA15]" [Pop+21a];
- **"CSA's Identity and Access Management for the Internet of Things - Summary Guidance": "**Extends the guidance on IoT Identity and Access Management (IAM) from [CSA15]. It provides a set of IAM related recommendations to support IoT adopters [CSA16]" [Pop+21a];
- **"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. Further, 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 [ENI20a]" [Pop+21a].

"Adopter Specific IoT Security Framework"

Based on the information disseminated by the author through the research paper [Pop+21a], 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 [CSA19b]. 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 [NIS04], FIPS PUB 200 [NIS06]) 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 [CSA19a]" [Pop+21a].

2.4.2. General IoT Security Best Practices

Based on the information disseminated by the author through the research paper [Pop+21a], this sub-subchapter provides an overview of the selected IoT security best practices which are "general in nature in terms of their applicability" [Pop+21a]. Each of these best practices is outlined below under its corresponding type-based category (i.e., "codes of practice", "guidelines", "frameworks") [Pop+21a].

"General IoT Security Codes of Practice"

Based on the information disseminated by the author through the research paper [Pop+21a], the selected general IoT security codes of practice focus on "secure IoT systems development lifecycle [DHS16], [IoT16]", and are outlined below:

- **"US 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 [DHS16]. These principles focus on four categories of IoT stakeholders (i.e., IoT developers, IoT manufacturers, service providers, and industrial and business-level consumers) [DHS16]. Garcia-Morchon et al. (2019) [Gar+19] describe this code of practice in a similar manner, and ECSO (2017) [ECS17] also provides a concise description covering the focus of this code of practice" [Pop+21a];
- **"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 [IoT16]" [Pop+21a].

"General IoT Security Guidelines"

All reviewed "general IoT security guidelines" are published by ENISA. Two of these are applicable to "sector-specific organizations [ENI17b], [ENI18b]", one guideline focuses on "secure IoT systems development lifecycle [ENI19b]", and another one focuses on "secure IoT supply chain [ENI20b]" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a], 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 [ENI17b]" [Pop+21a];

- **"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 [ENI18b]" [Pop+21a];
- **"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 [ENI19b]" [Pop+21a];
- **"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 [ENI20b]" [Pop+21a].

"General IoT Security Frameworks"

The selected "general IoT security frameworks" provide "strategic IoT security principles [Age20], [OTA18]" or "trustworthiness requirements [IIC16]" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a], these frameworks are outlined below:

- **"AgeLight's IoT Safety Architecture & Risk Toolkit v4.0":** "Provides 44 principles which are grouped into four categories (i.e., security by design, user identity & authentication, privacy, disclosures & transparency, related safety, privacy & 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 & costs, regulatory risk) while performing risk assessments against these recommended principles [Age20a]" [Pop+21a];

- **"IIC's Industrial Internet of Things Volume G4: Security Framework":** "This framework [IIC16] 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 [IIC16]. ECSO (2017) [ECS17] 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" [Pop+21a];
- **"OTA's IoT Security & Privacy Trust Framework v2.5":** "The framework [OTA18] is intended to serve as a risk assessment guide for developers, purchasers, and retailers [Gar+19]. It provides 44 strategic principles which are grouped into four key areas (i.e., security principles, user access & credentials, privacy, disclosures & transparency, notifications & related best practices), and where, each principle is flagged as either as required or recommended [OTA18]. ECSO (2017) [ECS17] also provides a concise description around the focus of this framework" [Pop+21a].

2.4.3. Manufacturer Specific IoT Security Best Practices

Based on the information disseminated by the author through the research paper [Pop+21a], this sub-subchapter provides an overview of the selected "manufacturer specific IoT security best practices" [Pop+21a]. Each of these best practices is outlined below under its corresponding type-based category (i.e., "standards", "guidelines") [Pop+21a].

"Manufacturer Specific IoT Security Standards"

Based on the information disseminated by the author through the research paper [Pop+21a], 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 [ETS20] consists of outcome-focused provisions (i.e., security and data protection) for developers and manufacturers to secure consumer IoT devices [Bra+19]. In addition, these provisions address constrained IoT devices. In addition, this standard provides a list of informative references [ETS20]" [Pop+21a];
- **"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 [NEM18]" [Pop+21a].

"Manufacturer Specific IoT Security Guidelines"

The selected "manufacturer specific IoT security guidelines" provide manufacturers with "security recommendations [BIT16], [NIS20a]", "baseline capabilities [CSD19]", or "principles for IoT devices [IEE17]" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a], the selected guidelines are outlined below:

- **"BITAG's Internet of Things (IoT) Security and Privacy Recommendations":** "This report [BIT16] addresses security and privacy issues of IoT devices [Gar+19], and it provides manufacturers with ten actionable security and privacy recommendations focused on consumer IoT devices [IEE17]. ECSO (2017) [ECS17] also provides a brief description around the focus of this guideline" [Pop+21a];
- **"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., [DCM18a], [ENI17b], [ETS20]) [CSD19]" [Pop+21a];
- **"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 [IEE17]" [Pop+21a];
- **"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 [NIS20a]" [Pop+21a].

2.4.4. Supplier Specific IoT Security Best Practices

Based on the information disseminated by the author through the research paper [Pop+21a], this sub-subchapter provides an overview of the selected "supplier specific IoT security best practices" [Pop+21a]. Each of these best practices is outlined below under its corresponding type-based category (i.e., "codes of practice", "guidelines", "frameworks") [Pop+21a].

"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 [DCM18a] and Australian Government [Com20]" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a], these “codes of practice” are outlined below:

- **“UK DCMS’s Code of Practice for Consumer IoT Security”:** “This code of practice [DCM18a] provides 13 prioritized guidelines for improving the security of consumer IoT products and associated services, and applies to device manufacturers, IoT service providers, mobile application developers and retailers [Gar+19]. In addition, for each IoT security guideline, the document lists the target stakeholders. In addition, this document (i.e., [DCM18a]) is supplemented by a comprehensive mapping document (i.e., [DCM18b]) which maps each recommended guideline against related IoT security recommendations, guidance and standards [Bra+19]” [Pop+21a];
- **“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 [DCM18a]. 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 [Com20]” [Pop+21a].

“Supplier Specific IoT Security Guidelines”

Based on the information disseminated by the author through the research paper [Pop+21a], 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 [AIO16]” [Pop+21a];
- **“US NHTSA’s Cybersecurity Best Practices for Modern Vehicles”:** “This document [NHT16] provides cybersecurity guidance for automotive industry and applies to motor vehicle and motor vehicle equipment designers, suppliers, manufacturers, alterers, and modifiers [Gar+19]” [Pop+21a].

“Supplier Specific IoT Security Frameworks”

Based on the information disseminated by the author through the research paper [Pop+21a], the selected “supplier specific IoT security frameworks” are outlined below:

- **“GSMA’s IoT Security Assessment Checklist Version 3.0”:** “This self-assessment checklist document [GSM18] 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 [Gar+19]. 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. Also, 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 [GSM18]. ECSO (2017) [ECS17] also mentions the self-assessment checklist and outlines the process for assessing IoT products, services, or components against this checklist" [Pop+21a];

- **"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) [ECS17], 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) [IoT20a]. 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) [IoT20a]. This framework is supplemented by a compliance checklist spreadsheet [IoT20b] to support the checkbox assessment exercise. A succinct description of this framework is also provided by Garcia-Morchon et al. (2019) [Gar+19]" [Pop+21a].

2.5. Conclusions

This chapter provided overviews of the key drivers for and enablers of cybersecurity risk management in organizations. With respect to the key drivers, the chapter provided an overview of the current cyber threat landscape and an overview of the cybersecurity regulatory landscape. Then, with respect to the key enablers, the chapter provided an overview of cybersecurity risk management frameworks and an overview of IoT security best practices.

First, this chapter aimed to enable the formation of a more holistic depiction of some of the most current cyber threats and provided an overview of the current cyber threat landscape by consolidating and categorizing the most frequently encountered cyber threats from seventeen relevant and well-renowned sources. Thus, following the review of the seventeen sources, the identified cyber threats were categorized into thirteen cyber threat categories (i.e., "malware attacks", "social engineering attacks", "denial of service (DoS)", "spam", "insider threat", "hacking attacks", "attacks on privacy and personal data", "cryptojacking", "targeted attacks on critical infrastructure", "supply chain attacks", "cyberpropaganda", and "legal and regulatory sanctions") that were outlined. Moreover, the study of the literature on the cyber threat landscape revealed the need for a cyber threat rating method that is dissociated from the elements (e.g., skill level, motive, opportunity) that induce uncertainty.

Then, this chapter provided an overview of the cybersecurity regulatory landscape by targeting key cybersecurity-related legislations and regulations pertaining to selected cybersecurity areas of statute (i.e., "the data protection and privacy" area and "critical infrastructure protection" area) under selected jurisdictions (i.e., European Union, Singapore, United States) and focusing exclusively on the statutes that were generally applicable and in force at the time of conducting the study on cybersecurity-related legislations. Hence, with respect to the European Union, one cybersecurity-related legislation was identified for each of the two cybersecurity areas of statute. Then, about Singapore, one cybersecurity-related legislation was identified for each of the two cybersecurity areas of statute. Finally, as for the United States, at the time of conducting the study on the cybersecurity-related legislations, there was no generally applicable data protection- and privacy-related legislation at federal level, and four cybersecurity-related legislations were identified for the critical infrastructure protection area. It is worth noting that the "NIST's Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)" was identified as being the by-product of the US legislation pertaining to the critical infrastructure protection area. Furthermore, the research study revealed the need for critical evaluations of selected cybersecurity-related legislations to establish the degree of commonality between them.

Afterwards, this chapter provided an overview of several well-renowned cybersecurity risk management frameworks by defining the "cybersecurity risk management framework" and by outlining some of the most widely adopted frameworks for managing cybersecurity risks. The frameworks were selected to be leveraged by any organization regardless of type, size, sector, or focus area, and grouped into three categories relevant for cybersecurity risk management (i.e., "cybersecurity-related frameworks", "generic risk management frameworks", and "IT-related frameworks"). The overview outlined ten "cybersecurity-related frameworks", three "generic risk management frameworks" and four "IT-related frameworks". Furthermore, the research study revealed the need for the critical evaluation of cybersecurity risk management frameworks to support decision making when it comes to framework selection.

Then, this chapter 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"). Further, this chapter provided a comprehensive overview of 25 selected IoT security best practices which were classified using the proposed taxonomic hierarchy and outlined under individual sub-subchapters that correspond to the four categories of IoT security best practices based on their applicability to specific groups of target audience. Thus, this overview outlined three guidelines and one framework for the adopter specific IoT security best practices, two codes of practice, four guidelines and three frameworks for the general IoT security best practices, two standards and four guidelines for the manufacturer specific IoT security best practices, and two codes of practice, two guidelines and two frameworks for the supplier specifc IoT security best practices. Furthermore, the study revealed the need for an IoT security risk management strategy reference model.

This chapter provided the following contributions:

- The determination and categorization of current cyber threats into thirteen up-to-date cyber threat categories along with the description of these cyber threat categories based on the investigation of seventeen relevant and well-renowned sources;
- An overview of the cybersecurity-related legislations and regulations pertaining to two cybersecurity areas of statute for three separate jurisdictions;
- The definition of the „cybersecurity risk management framework" term to enable a common understanding of this term;
- The identification, categorization, and description of frameworks relevant to cybersecurity risk management based on the study of the literature on the cybersecurity risk management;
- The development of a novel taxonomic hierarchy that classifies IoT security best practices based on their applicability to specific groups of target audience and type of IoT security best practice;

- The identification, classification, and description of IoT security best practices based on the study of the literature and the proposed taxonomic hierarchy.

The overviews presented in this chapter not only concretized in the aforementioned contributions of this chapter, but also made room for further thesis contributions which are outlined as part of the next chapters of this thesis.

3. EVALUATION OF CYBERSECURITY RISK MANAGEMENT DRIVERS

This chapter extends the research work on the cybersecurity risk management drivers outlined in Chapter 2, namely the cyber threat landscape and the cybersecurity regulatory landscape. Thus, this chapter aims to address current needs by providing relevant methods and critical evaluations based on these methods. First, with respect to the need for a cyber threat rating method that relies on measurable elements, the chapter provides a novel cyber threat rating method, applies this method to thirteen cyber threat categories to critically evaluate them, and it outlines the related work. Then, with respect to the need for critical evaluations of selected cybersecurity-related legislations to establish the degree of commonality between them, the chapter proposes a method for evaluating selected cybersecurity-related legislations, critically evaluates the in-scope cybersecurity-related legislations, and it outlines the related work.

Thus, this chapter addresses the following two thesis objectives:

- **Objective 5:** Propose a cyber threat rating method that aims to reduce the complexity and uncertainty attached to the existing threat rating methods and prioritize current cyber threats using this proposed method;
- **Objective 6:** Propose a method for evaluating key cybersecurity-related legislations to establish the degree of commonality between them from the perspective of the organizational understanding to managing cybersecurity risk and provide a critical evaluation of in-scope cybersecurity-related legislations based on the proposed method.

3.1. Applying a Cyber Threat Rating Method to Evaluate Cyber Threats

Nowadays, organizations are intrinsically linked to the cyberspace [Giu+21]. Moreover, while aiming to achieve efficiencies and gain commercial advantage over competitors, organizations are plunged into the digital transformation race which widens their attack surfaces, and in turn, opens new attack avenues for threat actors [Giu+21], [Jal+18]. Also, according to the WEF (2018b, 2019) [WEF18b], [WEF19] cyber risks are ever burgeoning, and are consolidating their position among the top ten global risks both in terms of probability of occurrence and of the corresponding cyber harm for individuals and society. In this context, "organizations are operating in a risky business environment which is subject to an ever-evolving cyber threat landscape" [Pop+19b]. Thus, to effectively de-risk their cybersecurity postures, "organizations need to form a thorough understanding of their cyber threat landscape through pragmatic cybersecurity risk assessments" [Pop+19b] entailing cyber threat profiling activities that leverage cyber threat rating methods [Pop+19b].

In this context, based on the information disseminated by the author through the research paper [Pop+19b] and the PhD report [Pop20], this subchapter extends the research work on cyber threat categories from Chapter 2.1 by providing a novel cyber threat rating method which is then applied to these cyber threat categories to prioritize them. This proposed method aims to reduce the complexity and uncertainty that characterize the existing threat rating methods which involve the evaluation of various attributes (e.g., skill level, motive, opportunity) [NIS12a], [OWA19] that are either unknown or hard to determine. Thus, the proposed method enables organizations to form a more holistic depiction of the possible extent of cyber harm associated with a cyber threat by relying upon the taxonomy of cyber harm advocated by Agrafiotis et al. (2018) [Agr+18] and supports the prioritization of cyber threats based on their potential to inflict cyber harm on organizations and their stakeholders [Pop+19b].

Hence, this subchapter provides a novel cyber threat rating method, and then before outlining the related work, the subchapter applies the proposed cyber threat rating method to the cyber threat categories outlined in the Chapter 2.1 to evaluate these cyber threat categories based on their possible extents of applicability to cyber harm.

3.1.1. Proposed Cyber Threat Rating Method

In order to support cybersecurity risk management in organizations, based on the information disseminated by the author through the research paper [Pop+19b] and the PhD report [Pop20], this sub-subchapter proposes a novel cyber threat rating method which relies on the latest taxonomy of organizational cyber harm developed by Agrafiotis et al. (2018) [Agr+18] and may be tailored by organizations to the profile of their environment while being used in conjunction with other methods. In this context, cyber harm refers to negative outcomes caused by cyber threats considering that harm is defined as "physical or other injury or damage" [Cam19]. Moreover, the proposed method aims to facilitate threat modelling by focusing exclusively on the model of the threats as identified by Shostack (2014) [Sho14] and by enabling the creation of a catalog of prioritized cyber threat categories [She+18], [Pop+19b].

The proposed method introduces x_k using the Equation (3.1) where x_k represents the set of in-scope cyber threat categories which vary according to the cyber threat landscape of each organization and C represents the cardinality of x_k [Pop20]:

$$x_k=\{\text{In-scope cyber threat categories}\}, \text{ where } k=[1..C] \text{ and } C=|x_k| \qquad (3.1)$$

The taxonomy of organizational cyber harm on which the cyber threat rating method relies upon includes the five main types with their sub-types of cyber harm advocated by Agrafiotis et al. (2018) (see Fig. 3.1) [Agr+18], [Pop+19b]. The main types consist of physical or digital harm caused to someone or something (i.e., the "Physical/Digital" type of cyber harm), financial or economic losses (i.e., the "Economic" type of cyber harm), psychological distress caused to an individual (i.e., the "Psychological" type of cyber harm), reputational damage inflicted on an entity (i.e., the "Reputational" type of cyber harm), and social damage (i.e., the "Social/Societal" type of cyber harm) [Agr+18], [Pop+19b]. Thus, to allow the linkage of the taxonomy of organizational cyber harm from Agrafiotis et al. (2018) to the formulas used in the proposed cyber threat rating method, the taxonomy is represented using the Equations from (3.2) to (3.7) [Pop20]:

- y_i represents the five types of cyber harm and n_i represents the number of sub-types for each of the types of cyber harm:

$$y_i = \left\{ \begin{array}{c} \text{"Physical / Digital", "Economic",} \\ \text{"Psychological", "Reputational",} \\ \text{"Social / societal"} \end{array} \right\}, \text{ where } i = [1..5],\ n_i = \{15,16,12,10,4\} \quad (3.2)$$

- y_{1j} represents the sub-types of the "Physical/Digital" type of cyber harm (i.e., y_1) and n_1 is the number of sub-types corresponding to this type of cyber harm (i.e., 15):

$$y_{1j} = \left\{ \begin{array}{c} \text{"Damaged or unavailable", "Destroyed", "Theft",} \\ \text{"Compromised", "Infected", "Exposed / leaked",} \\ \text{"Corrupted", "Reduced performance",} \\ \text{"Bodily injury", "Pain", "Loss of life",} \\ \text{"Prosecution", "Abuse", "Mistreatment",} \\ \text{"Identity theft"} \end{array} \right\}, \text{ where } j = [1..n_1] \qquad (3.3)$$

- y_{2j} represents the sub-types of the "Economic" type of cyber harm (i.e., y_2) and n_2 is the number of sub-types corresponding to this type of cyber harm (i.e., 16):

$$y_{2j} = \left\{ \begin{array}{c} \text{"Disrupted sales / turnover", "Reduced customers",} \\ \text{"Reduced profits", "Reduced growth",} \\ \text{"Reduced investments",} \\ \text{"Fall in stock price", "Theft of finances",} \\ \text{"Loss of finances / capital", "Regulatory fines",} \\ \text{"Investigation costs", "PR response costs",} \\ \text{"Compensation payments", "Extortion payments",} \\ \text{"Loss of jobs", "Scammed"} \end{array} \right\}, \text{ where } j = [1..n_2] \quad (3.4)$$

- y_{3j} represents the sub-types of the "Psychological" type of cyber harm (i.e., y_3) and n_3 is the number of sub-types corresponding to this type of cyber harm (i.e., 12):

$$y_{3j} = \left\{ \begin{array}{c} \text{"Confusion", "Discomfort", "Frustration",} \\ \text{"Worry / anxiety", "Feeling upset", "Depressed",} \\ \text{"Embarrassed", "Shameful", "Guilty",} \\ \text{"Loss of self-confidence", "Low satisfaction",} \\ \text{"Negative changes in perception"} \end{array} \right\}, \text{ where } j = [1..n_3] \qquad (3.5)$$

- y_{4j} represents the sub-types of the "Reputational" type of cyber harm (i.e., y_4) and n_4 is the number of sub-types corresponding to this type of cyber harm (i.e., 10):

$$y_{4j}=\left\{\begin{array}{c}\text{"Damaged public perception",}\\ \text{"Reduced corporate goodwill",}\\ \text{"Damaged relationship with customers",}\\ \text{"Damaged relationship with suppliers",}\\ \text{"Reduced business opportunities",}\\ \text{"Inability to recruit desired staff",}\\ \text{"Media scrutiny", "Loss of key staff",}\\ \text{"Loss/suspension of accreditations/certifications",}\\ \text{"Reduced credit scores"}\end{array}\right\}\text{, where } j = [1..n_4] \qquad (3.6)$$

- y_{5j} represents the sub-types of the "Social/Societal" type of cyber harm (i.e., y_5) and n_5 is the number of sub-types corresponding to this type of cyber harm (i.e., 4):

$$y_{5j}=\left\{\begin{array}{c}\text{"Negative changes in public perception",}\\ \text{"Disruption in daily life activities",}\\ \text{"Negative impact on nation",}\\ \text{"Drop in internal organization morale"}\end{array}\right\}\text{, where } j = [1..n_5] \qquad (3.7)$$

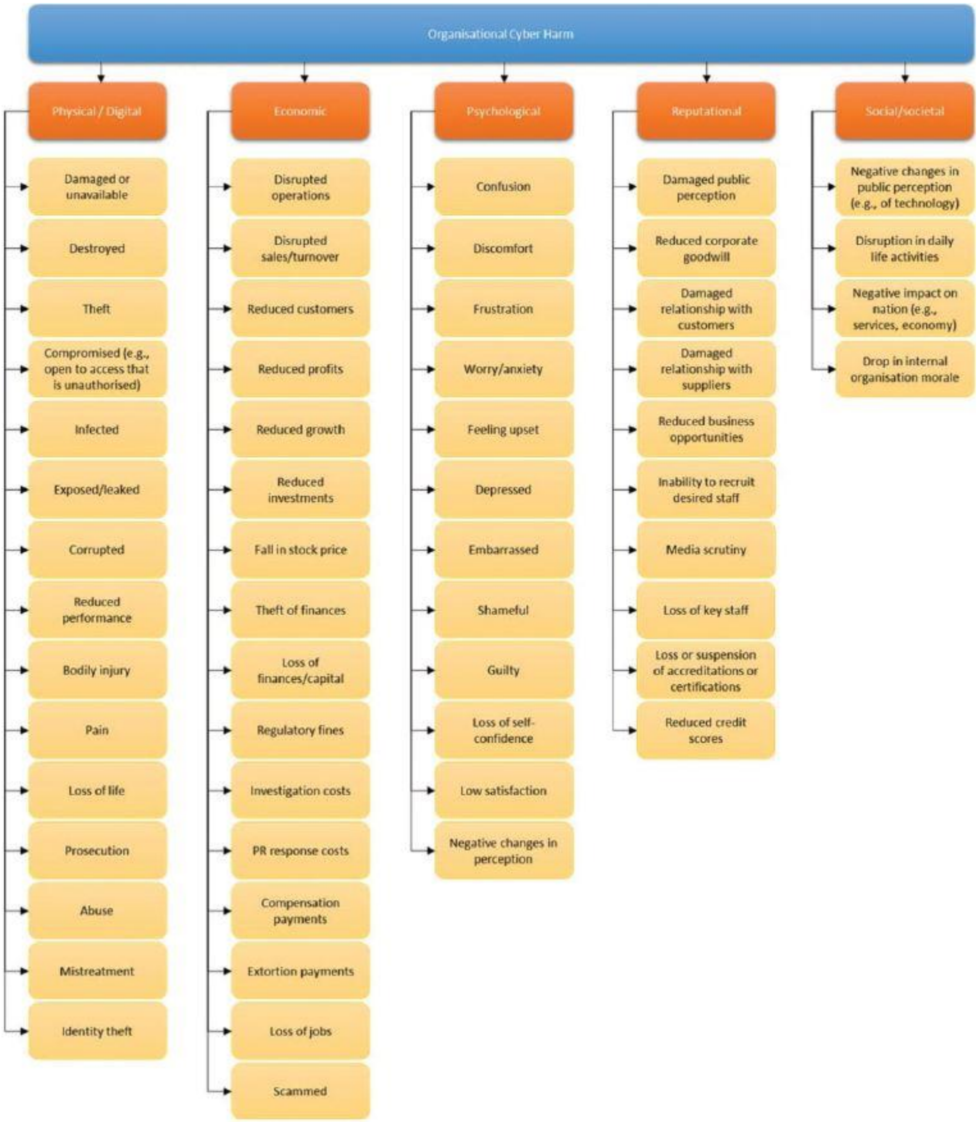


Fig. 3.1. Taxonomy of organizational cyber harms [Agr+18]

Then, the formulas used in the proposed cyber threat rating method is shown below [Pop20]:

- $\text{Rating}_{x_k}\left(y_{ij}\right)$ represents the rating of each cyber threat category of the set of in-scope cyber threat categories (i.e., x_k) against each of the sub-types (i.e., y_{ij}) of each type of cyber harm and n_i is the number of sub-types corresponding to each type of cyber harm (i.e., y_i):

$$\text{Rating}_{x_k}\left(y_{ij}\right)=\begin{cases}1, \text{ if the sub-type is applicable for } x_k \\ 0, \text{ otherwise}\end{cases}, \tag{3.8}$$

$$\text{where } k=[1..C],\ C=|x_k|,\ i=[1..5],\ j=[1..n_i]$$

Hence, the proposed cyber threat rating method involves rating each cyber threat category of the set of in-scope cyber threat categories against all sub-types of each type of organizational cyber harm with either "1" if the sub-type is applicable (i.e., when the cyber harm in question is possible considering a worst-case scenario), or "0" otherwise [Pop+19b], as shown in Equation (3.8). Subsequently, for each cyber threat category of the set of in-scope cyber threat categories, the ratings corresponding to the sub-types of each type of cyber harm are summed to score the extent to which the cyber threat category in question is potentially applicable to a specific type of cyber harm [Pop+19b] using the Equation (3.9) [Pop20]:

$$\text{Threat rating } (x_k) = \sum_{j=1}^{n_i}\text{Rating}_{x_k}\left(y_{ij}\right), \text{ where } k=[1..C],\ C=|x_k|,\ i=[1..5] \tag{3.9}$$

Then, as shown in Equation (3.10) for each cyber threat category of the set of in-scope cyber threat categories, the resulting scores are weighted by $1/n_i$, where n_i is the number of sub-types pertaining to each type of cyber harm [Pop+19b], [Pop20]:

$$\text{Weighted threat rating } (x_k) = \frac{1}{n_i}\sum_{j=1}^{n_i}\text{Rating}_{x_k}\left(y_{ij}\right), \text{ where } \sum_{1}^{n_i}\frac{1}{n_i}=100\% \tag{3.10}$$

These weighted scores enable the comparisons between the possible extents to which a specific cyber threat category of the set of in-scope cyber threat categories applies to different types of cyber harm, and between the in-scope cyber threat categories in relation to the possible extents to which they apply to a specific type of cyber harm [Pop+19b]. Finally, for each cyber threat category of the set of in-scope cyber threat categories, the resulting scores for the types of cyber harm are summed to indicate the extent to which that in-scope cyber threat category applies across all five types of cyber harm [Pop+19b] as shown in Equation (3.11) [Pop20]:

$$\text{Overall threat rating } (x_k) = \sum_{i=1}^{5}\sum_{j=1}^{n_i}\text{Rating}_{x_k}\left(y_{ij}\right) \tag{3.11}$$

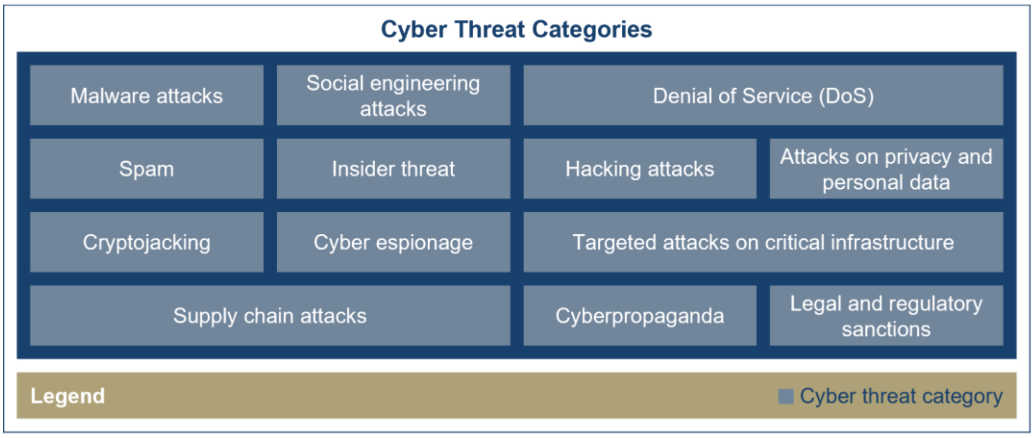
Further, as show in Equation (3.12), for each cyber threat category of the set of in-scope cyber threat categories, the resulting scores are weighted by 1/5, where 5 is the number of types of cyber harm [Pop+19b], [Pop20]:

$$\text{Weighted overall threat rating } (x_k)=\frac{1}{5}\sum_{i=1}^{5}\sum_{j=1}^{n_i}\text{Rating}_{x_k}\left(y_{ij}\right),\ \text{where } \sum_{1}^{5}\frac{1}{5}=100\% \quad (3.12)$$

These overall scores provide a mean to compare the in-scope cyber threat categories based on the possible extents of applicability to cyber harm considering the selected taxonomy of cyber harm. In addition, all weighted scores are expressed as percentages and are translated to qualitative ratings on a five-point scale (i.e., "Very Low": "0-20%", "Low": "21-40%", "Medium": "41-60%", "High": "61-80%", "Very High": "81-100%") [Pop+19b].

3.1.2. Evaluation of Cyber Threat Categories

Based on the information disseminated by the author through the research paper [Pop+19b], this sub-subchapter provides the critical evaluation of the thirteen cyber threat categories outlined in Chapter 2.1 using the threat ratings that resulted by applying the proposed cyber threat rating method to these cyber threat categories. Furthermore, these cyber threat categories are shown in Fig. 3.2.



Cyber Threat Categories

Malware attacks

Social engineering attacks

Denial of Service (DoS)

Spam

Insider threat

Hacking attacks

Attacks on privacy and personal data

Cryptojacking

Cyber espionage

Targeted attacks on critical infrastructure

Supply chain attacks

Cyberpropaganda

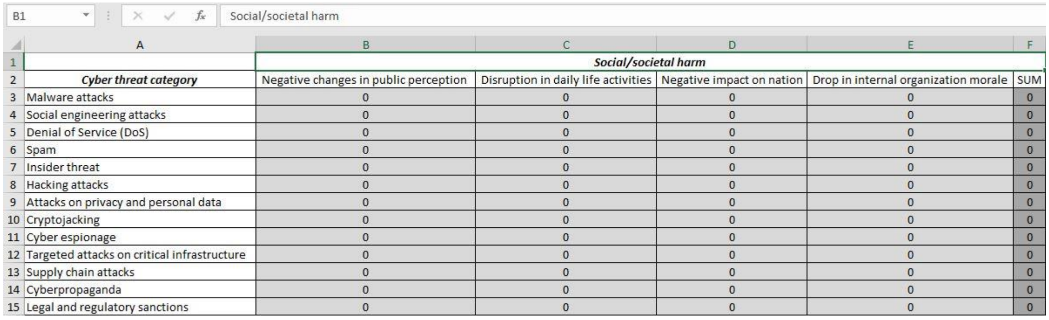
Legal and regulatory sanctions

Legend

▨ Cyber threat category

Fig. 3.2. Thirteen cyber threat categories

Thus, the application of the cyber threat rating method to the thirteen cyber threat categories relies on an Excel-based threat rating tool that was created to facilitate the calculus of threat ratings and the subsequent evaluation of the cyber threat categories. Fig. 3.3 shows an excerpt from the threat rating tool illustrating the input area corresponding to the category of social and societal harm prior to being populated [Pop+19b].



	A	B	C	D	E	F
1		*Social/societal harm*				
2	*Cyber threat category*	Negative changes in public perception	Disruption in daily life activities	Negative impact on nation	Drop in internal organization morale	SUM
3	Malware attacks	0	0	0	0	0
4	Social engineering attacks	0	0	0	0	0
5	Denial of Service (DoS)	0	0	0	0	0
6	Spam	0	0	0	0	0
7	Insider threat	0	0	0	0	0
8	Hacking attacks	0	0	0	0	0
9	Attacks on privacy and personal data	0	0	0	0	0
10	Cryptojacking	0	0	0	0	0
11	Cyber espionage	0	0	0	0	0
12	Targeted attacks on critical infrastructure	0	0	0	0	0
13	Supply chain attacks	0	0	0	0	0
14	Cyberpropaganda	0	0	0	0	0
15	Legal and regulatory sanctions	0	0	0	0	0

Fig. 3.3. Excerpt from the threat rating tool [Pop+19b]

Furthermore, the threat ratings are dependent on the analysis of cyber threat categories in relation to the possible extents to which these categories apply to cyber harm. Thus, Fig. 3.4 provides the outputs of the threat rating tool for each in-scope cyber threat category in relation to the types of cyber harm [Pop+19b].

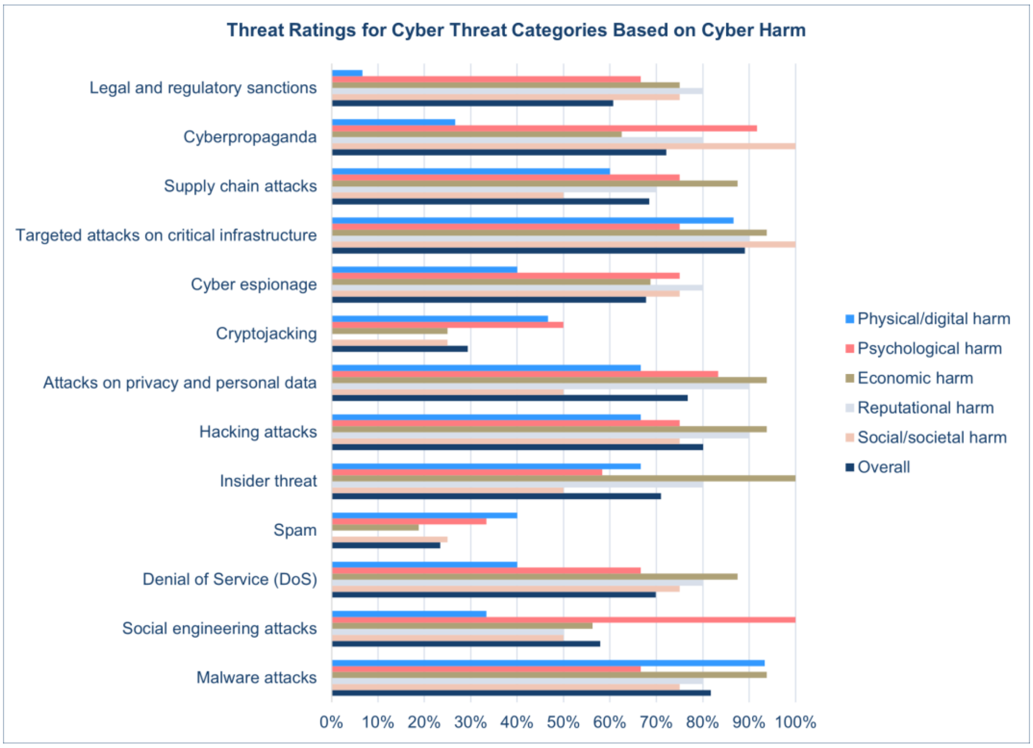


Fig. 3.4. Threat ratings for in-scope cyber threat categories based on cyber harm [Pop+19b]

First, the cyber threat categories that resulted overall as the most applicable to the types of cyber harm are "Targeted attacks on critical infrastructure", "Malware attacks", and "Hacking attacks", where all exhibit an overall threat rating of "Very High" (i.e., potentially a significant extent of applicability in relation to cyber harm).

Consequently, these cyber threat categories should be prioritized by organizations while conducting cybersecurity risk assessments. With respect to the "Targeted attacks on critical infrastructure", this cyber threat category exhibits "Very High" scores for four types of cyber harm (i.e., the "Physical/Digital", "Economic", "Reputational", and "Social/Societal" types of cyber harm) and a score of "High" for the "Psychological" type of cyber harm. Thus, from the perspective of a targeted attack on critical infrastructure, the "Psychological" type of cyber harm appears the least worrying type of cyber harm from all types. Regarding "Malware attacks", this cyber threat category presents "Very High" scores for two types of cyber harm, namely the "Physical/Digital" and the "Economic" types of cyber harm, and "High" ratings for all the remaining types. Hence, the threat ratings pertaining to malware attacks reveal that they are the most relevant for generating physical or digital damage and financial loss. And, in respect of "Hacking attacks", this category of cyber threat displays "Very High" applicability for the "Economic" and "Reputational" types of cyber harm, and "High" ratings for the rest. Thus, hacking attacks are very likely associated with the economic and reputational cyber harms [Pop+19b].

Second, there are seven categories of threats that exhibit overall ratings of "High", specifically "Attacks on privacy and personal data", "Cyberpropaganda", "Insider threat", "Denial of Service (DoS)", "Supply chain attacks", "Cyber espionage", and "Legal and regulatory sanctions". In effect, these cyber threat categories should also be of focal interest for organizations considering that a "High" rating indicates the potential for a fairly significant extent of applicability in relation to the whole spectrum of cyber harm. In terms of the "Attacks on privacy and personal data", this cyber threat category applies to "Very High" extents to three types of cyber harm (i.e., the "Psychological", "Economic", and "Reputational" types of cyber harm), to a "High" extent to the "Physical/Digital" type of cyber harm, and to a "Medium" or moderate extent to the "Social/Societal" type of cyber harm. Thus, this cyber threat category is the most relevant for the psychological, economic, and reputational cyber harms. Besides, it is worth noting that the threat ratings corresponding to the attacks on privacy and personal data reveal that this cyber threat category is more relevant at individual level rather than societal level. With respect to "Cyberpropaganda", the resulting ratings are "Very High" for both the "Psychological" and "Social/Societal" types of cyber harm, "High" associated with both the "Economic" and "Reputationa" types of cyber harm, and "Low" for the "Physical/Digital" type of cyber harm. Thus, cyberpropaganda is the most applicable to psychological and societal cyber harms, which may be precursors of other types of cyber harms. In terms of "Insider threat", this applies to a "Very High" extent to the "Economic" type of cyber harm, to "High" extents to both the "Physical/Digital" and "Reputational" types of cyber harm, moderate or "Medium" extents to both the "Psychological" and "Social/Societal" types of cyber harm. Next, in terms of "Denial of Service (DoS)", this cyber threat category displays a "Very High" score for the "Economic" type of cyber harm, "High" ratings for three types of cyber harm (i.e., "Psychological", "Reputational", and "Social/Societal"), and a "Low" rating for the "Physical/Digital" type of cyber harm. Then, in terms of "Supply chain attacks", this cyber threat category presents a "Very High" rating for the "Economic" type of cyber harm, "High" ratings for both the "Psychological" and "Reputational" types of cyber harm, and "Medium" ratings for both the "Physical/Digital" and "Social/Societal" types of cyber harm. Hence, the "Insider threat", "Denial of Service (DoS)", and "Supply chain attacks" threat categories are very likely to be linked to economic cyber harm. With respect to "Cyber espionage", this cyber threat category exhibits four "High" ratings (i.e., for the "Psychological", "Economic", "Reputational", and "Social/Societal" types of cyber harm) and a "Low" rating pertaining to the "Physical/Digital" type of cyber harm. And, regarding the "Legal and regulatory sanctions", this resembles "Cyber espionage" in terms of ratings except that this cyber threat category applies to a lesser extent to the "Physical/Digital" type of cyber harm, exhibiting a score of "Very Low" or negligible. Thus, "Cyber espionage" and "Legal and regulatory sanctions" are both less relevant for physical/digital type of cyber harm than for the other types of cyber harm [Pop+19b].

Then, "Social engineering attacks" is the only cyber threat category that has an overall rating of "Medium" (i.e., potentially a moderate extent of applicability across all types of cyber harm). Notwithstanding having the "Medium" threat rating, this cyber threat category should be seriously tackled by organizations considering that social engineering attacks may be attack vectors for other cyber threat categories [Pop+19b].

Afterwards, the remaining two categories of cyber threats (i.e., "Cryptojacking" and "Spam") resulted overall as the least applicable when considering all types of cyber harm, both displaying "Low" ratings (i.e., potentially a minor extent of applicability in view of all types of cyber harm). Thus, even though these cyber threat categories display "Low" ratings, they should not be overlooked by organizations as part of cybersecurity risk assessments as these threat ratings are not negligible. In respect of "Cryptojacking", this cyber threat category presents "Medium" ratings for both the "Physical/Digital" and "Psychological" types of cyber harm, "Low" ratings for both the "Economic" and "Social/Societal" types of cyber harm, and "Very Low" for the "Reputational" type of cyber harm. As for the "Spam" threat category, this exhibits three "Low" ratings (i.e., for the "Physical/Digital", "Psychological", and "Social/Societal" types of cyber harm), and two "Very Low" ratings (i.e., for the "Economic" and "Reputational" types of cyber harm). Therefore, both "Cryptojacking" and "Spam" do not appear to be relevant for reputational damage [Pop+19b].

Furthermore, Fig. 3.5 shows another consolidated view of the overall ratings for the thirteen cyber threat categories.

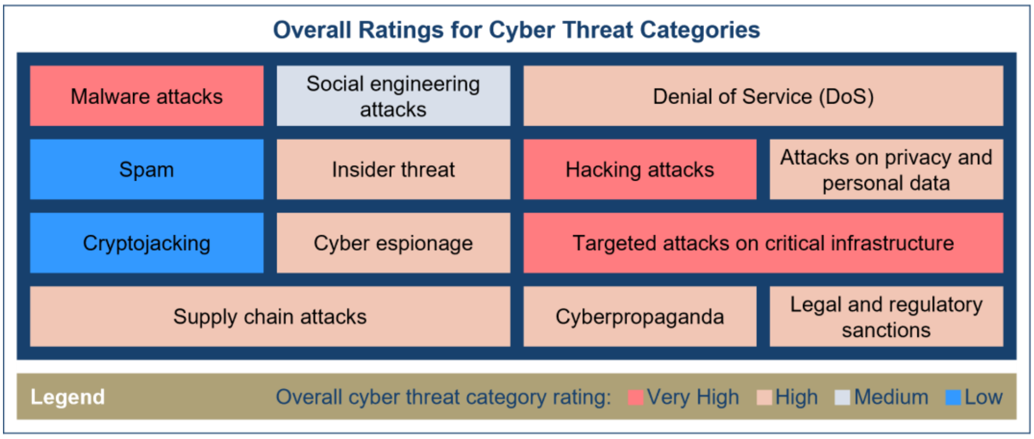

Overall Ratings for Cyber Threat Categories
Malware attacks
Social engineering attacks
Denial of Service (DoS)
Spam
Insider threat
Hacking attacks
Attacks on privacy and personal data
Cryptojacking
Cyber espionage
Targeted attacks on critical infrastructure
Supply chain attacks
Cyberpropaganda
Legal and regulatory sanctions
Legend
Overall cyber threat category rating: 🟥 Very High 🟧 High ⬜ Medium 🟦 Low

Fig. 3.5. Overall ratings for the thirteen cyber threat categories based on potential cyber harm

3.1.3. Related Work

Based on the information disseminated by the author through the research paper [Pop+19b], this sub-subchapter encompasses the related work in the context of the cyber threat rating methods, by reviewing literature related to the activities of threat prioritization [Pop+19b].

In this context, the selected thirteen cyber threat categories introduced in Chapter 2.1 are prioritized based on the taxonomy of cyber harm proposed by Agrafiotis et al. (2018) [Agr+18]. This cyber harm taxonomy was chosen as part of the proposed cyber threat rating method to allow a comprehensive depiction of the types of cyber harm [Agr+18] in relation to the in-scope cyber threat categories through the granularity provided by the sub-types of cyber harm (i.e., 15 sub-types for the "Physical/Digital" type of cyber harm, 12 sub-types for the "Psychological" type of cyber harm, 16 sub-types for the "Economic" type of cyber harm, 10 sub-types for the "Reputational" type of cyber harm, 4 sub-types for the "Social/Societal" type of cyber harm). Compared to Agrafiotis et al. (2018) [Agr+18] who suggested as future work the design of an asset-oriented model for detecting, measuring, predicting, and prioritizing cyber harm, the proposed cyber threat rating method leverages the cyber harm taxonomy to enable the visualization of the extents to which the in-scope cyber threat categories are potentially applicable to the types of cyber harm, and it is applied to the thirteen cyber threat categories to allow the evaluation of these cyber threat categories [Pop+19b].

In addition, other research works have provided means to calculate threat ratings as part of risk rating methodologies or risk assessment processes. For instance, the OWASP's risk rating methodology is based on threat agent factors (i.e., skill level, motive, opportunity, size) for estimating the likelihood of a successful attack [OWA19]. Another example for determining the likelihood of threat event initiation or occurrence is provided by NIST (2012a) [NIS12a], which takes into account capability, intent, and targeting characteristics for adversarial threat events, along with the historic frequency of the event for the non-adversarial threat events. In comparison with the threat rating methods proposed by NIST (2012a) [NIS12a] and by OWASP (2019) [OWA19], which are subject to a high degree of uncertainty and might affect the prioritization of risks [NIS12a], the proposed cyber threat rating method explores the potential applicability of the selected thirteen cyber threat categories to the types of cyber harm based on historical data and expert judgement [Pop+19b].

In this context, the proposed cyber threat rating method allows a detailed characterization and evaluation of the in-scope cyber threat categories based on the types of cyber harm, provides greater integration within the risk assessment process through the linkage of the in-scope cyber threat categories with the possible cyber harm, and alleviates the workload of the cyber risk assessors [Pop+19b] that want to use this method as part of their threat profiling works and maybe leverage some of the selected cyber threat categories that are prioritized.

3.2. Evaluation of Cybersecurity-Related Legislations

The global cybersecurity regulatory landscape is ever changing by rapidly growing in complexity and expanding the myriad of legal demands while organizations operating in one or multiple jurisdictions are striving to achieving a greater degree of compliance with the increasingly stringent legal requirements regarding cybersecurity risk management practices to preventing the rising sanctions for law infringements along with avoiding expensive litigations [Pon18], [Mar17], [May18], [Giu+21]. Moreover, compliance with applicable legislations can be a daunting and costly endeavor for organizations as some emerging legal requirements are converging with the existent ones inflicting organization-wide duplication, while others are inducing discrepancies that need to be carefully navigated depending on the organizational context [Mar17], [Del17b]. In this regard, based on the information disseminated by the author through the research paper [Pop+19a], this subchapter extends the research work on the cybersecurity regulatory landscape from Chapter 2.2 and aims to alleviate the degree of complexity associated with the regulatory compliance activities involved in the cybersecurity programs of organizations and to facilitate a pragmatic approach to attaining compliance, by focusing on organizational understanding of cybersecurity risk management and evaluating certain legislations and regulations to identify the degree of commonality between them [Pop+19a].

Hence, based on the information disseminated by the author through the research paper [Pop+19a], this subchapter offers a proposed method for evaluating key cybersecurity-related legislations, and then before outlining the related work, the subchapter provides the critical evaluation of the in-scope cybersecurity-related legislations "from the perspective of the organizational understanding to managing cybersecurity risk" [Pop+19a].

3.2.1. Proposed Method for Evaluating Cybersecurity-Related Legislations

Based on the information disseminated by the author through the research paper [Pop+19a], this sub-subchapter proposes a method for evaluating the in-scope cybersecurity-related legislations "from the perspective of organizational understanding to managing cybersecurity risk", which is based on the overview of the key cybersecurity-related legislations presented in Chapter 2.2 [Pop+19a]. Thus, considering the findings of a previous research work which reveal that "NIST CSF" not only sets the scene for integrated organization-wide risk management but also is the least prescriptive of the evaluated frameworks [Giu+21], "NIST CSF" appears the most suitable for evaluating the requirements of the in-scope legislations [Pop+19a]. Moreover, considering that the identify function of "NIST CSF" refers to an organization's ability to develop organizational understanding to enable cybersecurity risk management [NIS18a], this sub-subchapter proposes an evaluation method based on the "NIST CSF" to benchmark the legal requirements of the in-scope legislations against the underlying categories of the "NIST CSF Identify Function" [Pop+19a].

First, the proposed evaluation method introduces the underlying categories of the "NIST CSF Identify Function". Thus, the identify function of an organization comprises six underlying categories concerning the identification and management of data, personnel, devices, systems, and facilities relevant to achieving business objectives (i.e., "Asset Management"); the clarity around the mission, objectives, stakeholders, and activities (i.e., "Business Environment"); the policies, procedures, and processes governing cybersecurity risk management (i.e., "Governance"); the clarity around cybersecurity risk (i.e., "Risk Assessment"); the definition and use of priorities, constraints, risk tolerances, and assumptions to support integrated organization-wide risk management (i.e., "Risk Management Strategy"); the processes to manage supply chain risk (i.e., "Supply Chain Risk Management") [NIS18a], [Pop+19a].

Then, Table 3.1 shows the cybersecurity-related legislations outlined in Chapter 2.2, and maps each of these legislations and their references to the corresponding jurisdiction and area of statute.

Table 3.1. Selected cybersecurity-related legislations. Adapted from [Pop20]

Area	Jurisdiction	Name of Legislation	Reference
"Data protection and privacy"	"European Union"	"General Data Protection Regulation (Regulation (EU) 2016/679) of 27 April 2016"	[Off16a]
	"Singapore"	"Personal data protection act 2012"	[Gov12]
	"United States"	n/a*	n/a*
"Critical infrastructure protection"	"European Union"	"Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union"	[Off16c]
	"Singapore"	"Cybersecurity Act 2018"	[Gov18]
	"United States"	"The Critical Infrastructures Protection Act of 2001 of the PATRIOT Act"	[US01]
		"Executive Order for Improving critical infrastructure cybersecurity"	[The13a]
		"Presidential Policy Directive -- Critical Infrastructure Security and Resilience"	[The13b]
		"Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"	[The17]

*Note, n/a indicates that no generally applicable cybersecurity-related legislation was available

In this context, for the critical infrastructure protection area corresponding to the US, giving that the proposed evaluation method is based on the "NIST CSF" which is the by-product of the US legislation, the proposed evaluation method deliberately relies exclusively on the "NIST CSF" instead of considering specific US legislation for the critical infrastructure protection area with the purpose of reducing redundancy. Hence, the legislations and regulations considered in scope for the proposed evaluation method are the following [Pop+19a]:

- "General Data Protection Regulation (GDPR)"
- "Personal Data Protection Act 2012 (PDPA)"
- "Directive on Security of Network and Information Systems (NISD)"
- "Cybersecurity Act (CA)"

Furthermore, the proposed evaluation method introduces the definition of the value ratings (see Table 3.2). These five linguistic values will be used to represent the resulting outcomes of the critical evaluation and to indicate the extent to which the legislation in question corresponds to a particular category of the "NIST CSF Identify Function", as illustrated in Table 3.2 [Pop+19a].

Table 3.2. Definitions of the value ratings for evaluating the legislations [Pop+19a]

Value rating	Definition
"True"	A "True" value implies that "the statute comprises requirements that fully correspond to the NIST CSF category with no apparent discrepancies" [Pop+19a]
"Fairly True"	A "Fairly True" value means that "the statute comprises requirements that fairly correspond to the NIST CSF category with minor discrepancies" [Pop+19a]
"Partly True"	A "Partly True" value means that "the statute comprises requirements that partly correspond to the NIST CSF category with some discrepancies" [Pop+19a]
"Nearly False"	A "Nearly False" value means that "the statute comprises requirements that nearly deviate from the NIST CSF category with some similarities" [Pop+19a]
"False"	A "False" value implies that "the statute comprises requirements that deviate from the NIST CSF category with major discrepancies" [Pop+19a]

3.2.2. Evaluation of the In-Scope Cybersecurity-Related Legislations

Based on the proposed evaluation method introduced in Chapter 3.2.1 and on the information disseminated by the author through the research paper [Pop+19a], this sub-subchapter provides the critical evaluation of the in-scope cybersecurity related legislations pertaining to "data protection and privacy" and "critical infrastructure protection" areas from the selected jurisdictions by "focusing on the enablers for organizational understanding with respect to managing cybersecurity risk" [Pop+19a].

Consequently, Table 3.3 summarizes the findings of the evaluation for each selected legislation in relation to the above categories of the identify function [Pop+19a].

Table 3.3. Results of the evaluation of the in-scope legislations [Pop+19a]

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

Unique ID.	NIST CSF Category	GDPR	PDPA	NISD	CA
"ID.SC"	"Supply Chain Risk Management"	Fairly True	Nearly False	Fairly True	Nearly False

Following Table 3.3, this sub-subchapter presents the critical evaluation of the in-scope cybersecurity-related legislations for the underlying categories of the "NIST CSF Identify Function" [Pop+19a].

"Asset Management (ID.AM)": Both "CA" and "NISD" comprise requirements related to inventorying the critical infrastructure systems involving understanding technologies components and service dependencies, and "CA" also addresses record keeping obligations with respect to providers of licensable cybersecurity services [Off16c], [Gov18], [Sha+16b], [Con19], [Cro18]. Furthermore, "PDPA" merely focuses on keeping records of how personal data is used or disclosed by the organization [Gov12] whereas "GDPR" requires controllers and processors to maintain a record of processing activities under their responsibility and imposes greater protection for processing of special categories of personal data [Off16a], [CMS18], [Ver18a], [IAP19], [Pop+19a]. Thus, the requirements of "CA" and "NISD" fully correspond to this category with no apparent discrepancies, the "GPDR's" requirements fairly correspond to this category with minor discrepancies, and the "PDPA's" requirements nearly deviate from this category with some similarities.

"Business Environment (ID.BE)": While "PDPA" prescribes data protection and retention requirements on data intermediaries processing personal data and does not impose obligations to address cybersecurity risk under the contractual obligations with data intermediaries, the "GDPR" clearly prescribes the stipulation of appropriate safeguards within the contractual agreements between the controllers and processors [Gov12], [Off16a], [CMS18]. Furthermore, while "CA" is not prescriptive with respect to measures to be taken by owners to ensure the cybersecurity of "CII" and merely requires the identification of interconnections or communications between any computer or computer systems with the "CII", "NISD" requires the identification of dependencies and resilience obligations to support the delivery of critical services through appropriate measures to ensure service continuity [Gov18], [Off16c], [Pop+19a]. Thus, the "NISD'"s requirements fairly correspond to this category with minor discrepancies, the requirements of "CA" and "GPDR" partly correspond to this category with some discrepancies, and the "PDPA's" requirements nearly deviate from this category with some similarities.

"Governance (ID.GV)": "GDPR" requires controllers to adopt data protection policies and promote data protection, imposes on controllers and processors adherence to binding corporate rules when engaging in cross-border personal data transfers involving third countries, imposes the designation of a data protection officer where applicable, clearly states the responsibilities of controllers and processors referencing their approved codes of conduct or certification mechanisms and contractual agreements governing the processing respectively, along with powers of competent supervisory authorities [Off16a], [Ver18a]. And, "PDPA" prescribes organizations to develop, implement, publish and communicate policies and practices pursuant to "PDPA", imposes the designation of one or more individuals responsible for data protection, makes organizations accountable for personal data including data protection and imposes data protection and retention obligations on data intermediaries [Gov12]. Furthermore, "CA" requires owners of "CII" to comply with cybersecurity codes of practice and standards of performance issued by the

Commissioner, prescribes responsibilities for the licensable cybersecurity services, along with duties for owners of "CII" such as undergoing compliance audits of "CII" carried out by an approved auditor, and imposes on owners of "CII" obligations to establish processes for the purposes of detecting cybersecurity threats and incidents in respect of "CII", along with clear sanctions for not complying with "CA" [Gov18]. Additionally, "NISD" requires "OESs" and "DSPs" having documented security policies, prescribes the responsibilities of "OESs" and "DSPs", the elements of the risk management process, and requires Member States to establish the rules on penalties applicable for law infringements [Off16c], [Pop+19a]. Thus, the NISD's requirements fully correspond to this category with no apparent discrepancies, the "GPDR's" requirements fairly correspond to this category with minor discrepancies, and the requirements of "CA" and "PDPA" nearly deviate from this category with some similarities.

"Risk Assessment (ID.RA)": Although neither the "NISD", nor the "CA" are specifically prescribing the manner for carrying out cybersecurity risk assessments, the NISD requires the taking of appropriate and proportionate measures to manage the risks and "CA" requires owners of "CII" to conduct cybersecurity risk assessments annually [Off16c], [Gov18]. Additionally, while "PDPA" merely prescribes the making of reasonable security arrangements to prevent risks to data under the organization's control, "GDPR" clearly prescribes carrying out a data protection impact assessment prior to engaging in processing that pose a high risk to the rights and freedoms of natural persons, and implementing a process for regularly assessing the effectiveness of controls for ensuring the security of the processing [Gov12], [Off16a], [CMS18], [Pop+19a]. Thus, the requirements of "CA" and "NISD" fairly correspond to this category with minor discrepancies, the "GPDR's" requirements partly correspond to this category with some discrepancies, and the "PDPA's" requirements nearly deviate from this category with some similarities.

"Risk Management Strategy (ID.RM)": As opposed to "GDPR" which requires controllers and processors to ensure a level of security appropriate to the risk via appropriate safeguards on processing systems and services to maintain their "CIA" triad and resilience properties, "PDPA" merely prescribes for organizations to making reasonable security arrangements to prevent risks regarding personal data [Gov12], [Off16a], [CMS18]. Further, while "CA" merely makes reference to risk management components rather than clearly prescribing the cybersecurity risk management measures to be adopted by the owners of "CII", the "NISD" sets forth that all EU Member States should promote and achieve a culture of risk management through appropriate regulatory requirements having the "OESs" and "DSPs" responsible for ensuring that appropriate and proportionate safeguards are in place to manage the risks posed to the security of their networks and information systems [Off16c], [Gov18], [Pop+19a]. Thus, the "NISD's" requirements fairly correspond to this category with minor discrepancies, the "GPDR's" requirements partly correspond to this category with some discrepancies, and the requirements of the "CA" and "PDPA" nearly deviate from this category with some similarities.

"Supply Chain Risk Management (ID.SC)": "PDPA" imposes notification of purposes for the collection, use or disclosure of the personal data prior to data collection by third parties to allow the organization to establish the lawfulness of the data disclosure, and, in respect of personal data processing by third parties, it prescribes merely data protection and retention obligations on data intermediaries rather than making them accountable for the processing of personal data [Gov12]. On the other hand, the "GDPR" requirements with respect to supply chain risk management are more comprehensive clearly delineating the responsibilities of the controllers and processors, restricting the making of agreements only to processors providing sufficient guarantees to implement safeguards as deemed appropriate by the "GDPR", and prescribing the governance of the processing under a binding contract incorporating, inter alia, controller's right to audits and security obligations on the processor including ensuring a level of security commensurate with risk [Off16a], [IAP19]. Besides, with respect to cyber supply chain risk management, the "CA" provides a licensing framework for the providers of licensable cybersecurity services (i.e., managed security operations centre monitoring service and penetration testing service), but it does not specifically impose obligations on owners of "CII" other than ensuring the cybersecurity of the "CII" and notifying the Commissioner of the occurrence of relevant cybersecurity incidents [Gov18]. Nevertheless, among others, the "NISD" addresses the need for "OESs" and "DSPs" to ensuring the security of critical infrastructure systems against cybersecurity risks irrespective of whether the maintenance is performed internally or outsourced to an external supplier, and imposes obligations on "DSPs" for "OESs" to notify the operators about any significant impact on the continuity of the essential services [Off16c], [Cro18], [Pop+19a]. Thus, the requirements of the "GDPR" and "NISD" fairly correspond to this category with minor discrepancies and the requirements of the "CA" and "PDPA" nearly deviate from this category with some similarities.

3.2.3. Related Work

Based on the information disseminated by the author through the research paper [Pop+19a], this sub-subchapter encompasses the related work in the context of the cybersecurity legislations and regulations relevant to the selected areas of statute under the three jurisdictions addressed in this chapter [Pop+19a].

In this context, much of the literature pays particular attention to addressing cybersecurity laws in silos [Joh+14], for instance around "GDPR" [Cob+18], [Sir+18], [Eur18b], [ICO18] and "NISD" [Cro18]. Thus, this subchapter takes a more holistic approach by addressing more than one law [Pop+19a].

Moreover, other research works have provided an overview of a set of cybersecurity-related laws from a single jurisdiction, whereas this subchapter covers three key jurisdictions by evaluating the in-scope laws. For instance, FireEye and Marsh & McLennan Companies (2017) [Fir+17] described the key EU cybersecurity legislation and regulation (i.e., "GDPR" and "NISD") as part of their report which provided the organizations' cyber preparedness across EU. With respect to the US, among others, Kosseff (2018b) [Kos18b] defined the cybersecurity law, examined the gaps in current US cybersecurity law, and suggested starting points for improvements. In this view, similar to Kosseff's (2018b) [Kos18b] approach which focused on specific categories of laws associated with cybersecurity, this subchapter covers two cybersecurity-related areas of statute that are essential to triggering cybersecurity risk management in organizations, and it evaluates the in-scope cybersecurity laws pertaining to these areas of statute under each of the key cybersecurity jurisdictions [Pop+19a].

In addition, other studies have investigated only the statutes related to a single cybersecurity area covering multiple jurisdictions. DLA Piper (2018) [DLA18] provided an overview of key laws and regulations pertaining to data protection and privacy area from nearly 100 different jurisdictions. As opposed to these research works which have only focused on the laws applicable to one cybersecurity area from multiple jurisdictions, this subchapter evaluates some of the key statutes pertaining to two cybersecurity areas from three jurisdictions selected based on their cybersecurity maturity level [Pop+19a].

Furthermore, as compared with the existent works which have been carried out on addressing the laws pertaining to multiple cybersecurity areas from multiple jurisdictions [Glo17], [Häg+17], [Joh+14], [Rav+18], [Hog18], [Law17], [Sun+18], this subchapter provides a critical evaluation of in-scope statutes against the categories of the identify function of "NIST CSF" [Pop+19a].

In addition, much of the research up to now has been focused on providing cross-references of "GDPR" to different cybersecurity-related frameworks including, among others, the cross-references to "NIST CSF" as presented in Ref. [Ver18a], updating the informative references from "NIST CSF" with "GDPR" as outlined in Ref. [Con19], providing a high level evaluation of the "NISD" against the functions of "NIST CSF" as performed by Shackelford et al. (2016), providing a comparison between "GDPR" and "PDPA" as captured in Ref. [CMS18], or comparing "GDPR" with "ISO27001" to identify common grounds and overlaps between the two as provided in Ref. [IAP19]. Thus, no previous research work has been found at the time of conducting this study that evaluated all four cybersecurity laws (i.e., "GDPR", "NISD", "PDPA", "CA") against the categories of the identify function of "NIST CSF" [Pop+19a].

3.3. Conclusions

This chapter extended the research work on the cybersecurity risk management drivers (i.e., the cyber threat landscape and the cybersecurity regulatory landscape) outlined in Chapter 2 by proposing and applying a cyber threat rating method to critically evaluate the thirteen cyber threat categories and by proposing and applying an evaluation method to critically evaluate the in-scope cybersecurity-related legislations.

First, this chapter aimed to support the prioritization of cyber threats based on their potential to inflict cyber harm on organizations and their stakeholders and to enable the formation of a more holistic depiction of some of the most current cyber threats by addressing the need for a cyber threat rating method based on measurable elements. Thus, this chapter provided a novel cyber threat rating method which allows the analysis of cyber threat categories, the estimation of the extents of their applicability to cyber harm based on the latest taxonomy of organizational cyber harm, and the prioritization of the in-scope cyber threat categories. The taxonomy of cyber harm consists of the "Physical/Digital", "Economic", "Psychological", "Reputational", and "Social/Societal" types of cyber harm with fifteen, sixteen, twelve, ten, and four sub-types of cyber harm, respectively. Moreover, this method allows the calculus associated with the determination of the extent to which a certain cyber threat category is potentially applicable to a specific and across all types of cyber harm.

Then, this cyber threat rating method was applied to the thirteen cyber threat categories from Chapter 2 using an Excel-based threat rating tool. Hence, each of these cyber threat categories was considered in relation to each sub-type of each type of cyber harm and each of the corresponding observations was assigned a value of either "1" if the sub-type appeared to be applicable or "0" otherwise, before processing the results across each and all five types of cyber harm.

Furthermore, this chapter provided a critical evaluation of the thirteen cyber threat categories based on their threat ratings that resulted from applying the cyber threat rating method, which allowed the prioritization of these cyber threat categories.

This evaluation revealed that three, seven, one, and two cyber threat categories exhibit "Very High", "High", "Medium", and "Low" extents of applicability to cyber harm, respectively. About the "Very High" extent of applicability to cyber harm, the "Targeted attacks on critical infrastructure", "Malware attacks", and "Hacking attacks" threat categories resulted in having scores that match the "Very High" rating. Thus, these cyber threat categories should be at the top of the list when it comes to cyber threats. Then, this chapter provided the findings derived from the review of the related work. Hence, one of the main findings was that the proposed cyber threat rating method leverages the latest taxonomy of cyber harm in new ways that were not previously explored.

Afterwards, this chapter aimed to alleviate the degree of complexity associated with achieving organizational compliance with cybersecurity-related legislations and regulations by addressing the need for critical evaluations of selected cybersecurity-related legislations to establish the degree of commonality between them and support a pragmatic approach to attaining regulatory compliance for organizations striving to prevent the sanctions and costly lawsuits following law infringements. In this context, this chapter proposed a method for evaluating selected cybersecurity-related legislations from the perspective of organizational understanding of cybersecurity risk management, which is based on the overview of the key cybersecurity-related legislations of the key cybersecurity jurisdictions from Chapter 2.2 and on the "NIST CSF Identify Function".

Then, this chapter critically evaluated the in-scope cybersecurity-related legislations (i.e., "the General Data Protection Regulation – GDPR", "Personal Data Protection Act 2012 – PDPA", "Directive on Security of Network and Information Systems – NISD", "Cybersecurity Act – CA") against the six categories of the "NIST CSF Identify Function" (i.e., "Asset Management", "Business Environment", "Governance", "Risk Assessment", "Risk Management Strategy", "Supply Chain Risk Management"). Thus, with respect to the "Asset Management" category, the requirements of "CA" and "NISD" fully correspond to this category with no apparent discrepancies and the "GPDR's" requirements fairly correspond to this category with minor discrepancies. About the "Business Environment" category, the "NISD's" requirements fairly correspond to this category with minor discrepancies. Regarding the "Governance" category, the "NISD's" requirements fully correspond to this category with no apparent discrepancies and the "GPDR's" requirements fairly correspond to this category with minor discrepancies. In terms of the "Risk Assessment" category, the requirements of "CA" and "NISD" fairly correspond to this category with minor discrepancies. About the "Risk Management Strategy" category, the "NISD's" requirements fairly correspond to this category with minor discrepancies. As for the "Supply Chain Risk Management" category, the requirements of the "GDPR" and "NISD" fairly correspond to this category with minor discrepancies. Afterwards, this chapter provided the related work, which revealed that, at the time of conducting the study, no previous research work was found that evaluated all four cybersecurity-related laws against the "NIST CSF Identify Function".

This chapter provided the following contributions:

- The design of a novel cyber threat rating method and the creation of a threat rating tool;
- The application of the proposed cyber threat rating method to thirteen cyber threat categories for evaluating these cyber threat categories;
- The critical evaluation of the thirteen cyber threat categories based on their possible extents of applicability to cyber harm;
- A comparison of the proposed threat rating method with the related work;

- The design of a new method for evaluating selected key cybersecurity-related legislations;
- The critical evaluation of the in-scope cybersecurity-related legislations to establish the degree of commonality between them from the perspective of organizational understanding to managing cybersecurity risk;
- An analysis of the related work relevant to the evaluation of cybersecurity-related legislations.

4. EVALUATION OF CYBERSECURITY RISK MANAGEMENT FRAMEWORKS

Based on the information disseminated by the author through the research paper [Giu+21] and the PhD report [Pop20], this chapter builds on the overview of cybersecurity risk management frameworks provided in Chapter 2.3. Thus, given the frameworks are the nucleus of cybersecurity risk management programmes, this chapter aims to address the paucity of studies providing a comprehensive characterization of frameworks relative to each other "to support decision-making with respect to framework selection, facilitate pragmatic implementation of cybersecurity programmes, and help organizations better cope with cybersecurity risks" [Giu+21].

First, the chapter proposes a methodology for evaluating the in-scope frameworks and then critically evaluates these cybersecurity frameworks based on the proposed methodology. Finally, the chapter outlines the related work relevant to cybersecurity risk management frameworks through a detailed analysis of the existing literature by delving into the related studies with a narrower and a partly different scope than the scope of the evaluation methodology proposed in this chapter.

Thus, this chapter addresses the following thesis objective:

- **Objective 7:** Propose a methodology for evaluating cybersecurity risk management frameworks and provide a critical evaluation of in-scope cybersecurity risk management frameworks based on the proposed methodology.

4.1. Proposed Methodology for Evaluating the In-Scope Frameworks

Based on the information disseminated by the author through the research paper [Giu+21] and the PhD report [Pop20], this subchapter provides the proposed methodology for evaluating the in-scope cybersecurity risk management frameworks (see Fig. 4.1). Thus, the proposed evaluation methodology involves identifying, analysing, and comparing the in-scope cybersecurity risk management frameworks as part of the three phases of this methodology. These three phases of the proposed methodology are illustrated in Fig. 4.1 along with the corresponding inputs and outputs [Pop20].

The proposed methodology enables the characterization of each of the in-scope frameworks and aims to provide a consolidated view over some of the main characteristics of all in-scope frameworks. It is worthwhile noting that the proposed methodology was not crafted as a means of selecting one of the in-scope frameworks as a better alternative over the others. Thus, this evaluation methodology can be further extended to provide a way of establishing which of the selected frameworks is better [Pop20].

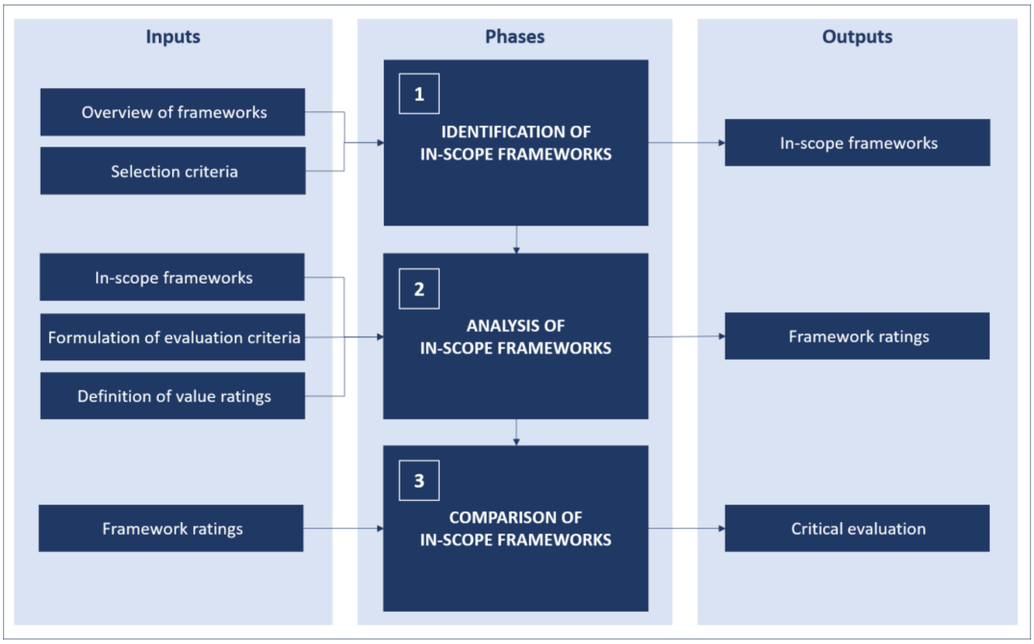

Inputs
Phases
Outputs
Overview of frameworks
Selection criteria
1
IDENTIFICATION OF IN-SCOPE FRAMEWORKS
In-scope frameworks
In-scope frameworks
Formulation of evaluation criteria
Definition of value ratings
2
ANALYSIS OF IN-SCOPE FRAMEWORKS
Framework ratings
Framework ratings
3
COMPARISON OF IN-SCOPE FRAMEWORKS
Critical evaluation

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

The first phase of the proposed evaluation methodology involves the identification of the in-scope frameworks for the evaluation [Pop20]. From the range of cybersecurity risk management frameworks outlined in Chapter 2.3, the proposed methodology applies the selection criteria of "focusing merely on those specific frameworks that are free of charge with readily available documentation as these characteristics are essential for making this evaluation possible" [Giu+21].

Further, the second phase of the proposed evaluation methodology involves the analysis of in-scope frameworks [Pop20]. To support the analysis of each of the selected frameworks, the formulation of the evaluation criteria is outlined (see Fig. 4.2, Table 4.1), and then the value ratings are defined (see Table 4.2) [Pop20]. Both the evaluation criteria and the value ratings are used for examining the in-scope frameworks to determine the framework ratings [Giu+21].

Formulating the evaluation criteria is an essential step while addressing Multiple Attribute Decision Making (MADM) problems [Tze+11]. This step is an input for the proposed evaluation methodology where a hierarchical structure is proposed for evaluating the in-scope cybersecurity risk management frameworks [Pop20]. Fig. 4.2 shows the proposed hierarchical structure for evaluating the in-scope cybersecurity risk management frameworks [Pop20]. Thus, the study focused on 7 dimensions and 13 evaluation criteria. In this view, the selected evaluation criteria are based on "several fundamental elements relevant to emphasize similarities and differences between the aforementioned cybersecurity risk management frameworks", including the following dimensions: "definition, purpose, and type of the cybersecurity risk management framework (see Chapter 2.3)", "compatibility with other frameworks and standards or regulatory requirements", "key elements pertaining to the risk management process (i.e., the analytic approach [NIS12a], risk treatment elements)", "supporting documentation available", and "continuous framework improvement" [Giu+21]. Also, for ease of use, each evaluation criterion is given a unique identifier (i.e., "Unique ID.") [Giu+21].

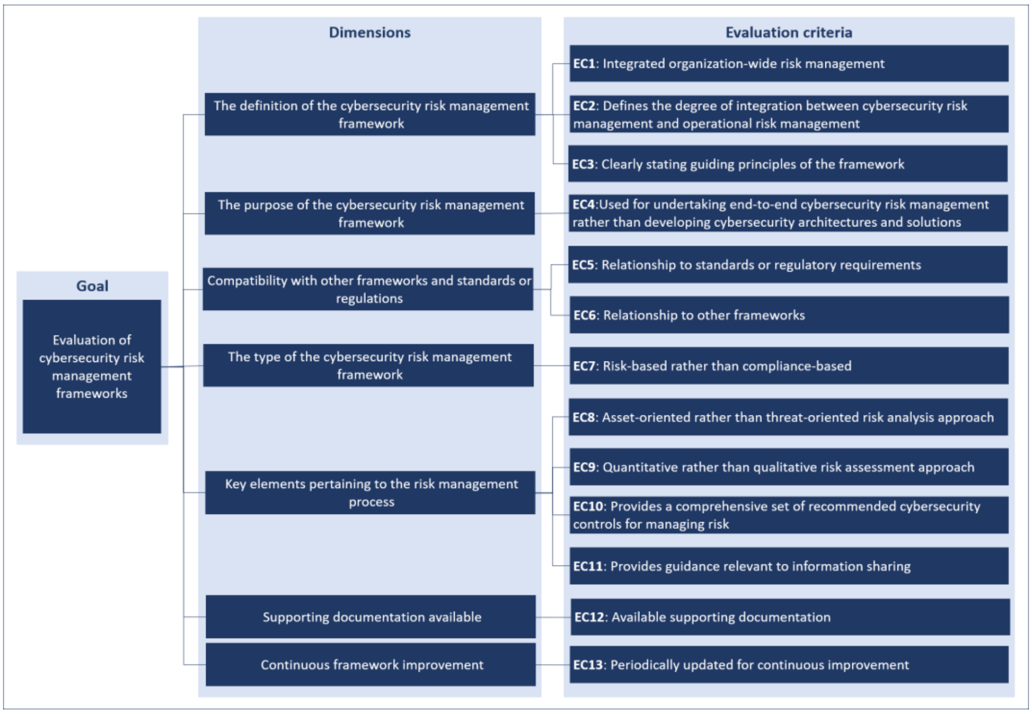

Goal
Evaluation of cybersecurity risk management frameworks
Dimensions
The definition of the cybersecurity risk management framework
The purpose of the cybersecurity risk management framework
Compatibility with other frameworks and standards or regulations
The type of the cybersecurity risk management framework
Key elements pertaining to the risk management process
Supporting documentation available
Continuous framework improvement
Evaluation criteria
EC1: Integrated organization-wide risk management
EC2: Defines the degree of integration between cybersecurity risk management and operational risk management
EC3: Clearly stating guiding principles of the framework
EC4:Used for undertaking end-to-end cybersecurity risk management rather than developing cybersecurity architectures and solutions
EC5: Relationship to standards or regulatory requirements
EC6: Relationship to other frameworks
EC7: Risk-based rather than compliance-based
EC8: Asset-oriented rather than threat-oriented risk analysis approach
EC9: Quantitative rather than qualitative risk assessment approach
EC10: Provides a comprehensive set of recommended cybersecurity controls for managing risk
EC11: Provides guidance relevant to information sharing
EC12: Available supporting documentation
EC13: Periodically updated for continuous improvement

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

Thus, based on "framework definition", the first criterion of the evaluation (i.e., "EC1") is related to "whether the assessed cybersecurity risk management framework facilitates integrated organization-wide risk management" [Giu+21]. The second evaluation criterion (i.e., "EC2") is used for "establishing whether the framework under consideration defines the degree of integration between cybersecurity risk management and operational risk management activities" [Giu+21]. The next evaluation criterion (i.e., "EC3") is concerned with "determining whether the selected framework is clearly stating its guiding principles" [Giu+21]. Further, another evaluation criterion (i.e., "EC4") relates to "the extent to which the purpose of the framework in question is more closely relevant to undertaking end-to-end cybersecurity risk management as opposed to developing cybersecurity architectures and solutions" [Giu+21]. Then, the next two criteria (i.e., "EC5", "EC6") (i.e., "relationship to standards or regulatory requirements", "relationship to other frameworks") are selected to "establish whether the assessed frameworks are compatible with other relevant frameworks and standards or regulatory requirements" [Giu+21]. Afterwards, the subsequent criterion selected (i.e., "EC7") aims to "inform whether the type of the framework in question aligns with a risk-based as opposed to a compliance-based (i.e., a checkbox cybersecurity mindset) approach" [Giu+21]. Then, the following two criteria (i.e., "EC8", "EC9") (i.e., "asset-oriented rather than threat-oriented risk analysis approach", "quantitative rather than qualitative risk assessment approach") relate to "the nature of the approach adopted while conducting risk assessments (see the description of asset-oriented and threat-oriented terms provided as part of the CIS RAM from Chapter 2.3.3) along with risk measurement aspects [Nur+17]" [Giu+21]. Furthermore, two evaluation criteria (i.e., "EC10", "EC11") outline "risk treatment items relevant to the assessed frameworks, specifically whether the frameworks provide a comprehensive set of recommended cybersecurity controls and guidance relevant to information sharing activities for risk management" [Giu+21]. In addition, this evaluation explores "whether the assessed frameworks come together with available supporting documentation (procedures, templates, methods, case studies, etc.)" (i.e., "EC12"), and ultimately "whether they are periodically updated for continuous improvement" (i.e., "EC13") [Giu+21].

Table 4.1. Evaluation criteria for evaluating the in-scope frameworks [Giu+21]

Unique ID.	Evaluation Criterion	Description
"EC1"	"Integrated organization-wide risk management" [Giu+21]	To indicate "whether the assessed cybersecurity risk management (RM) framework facilitates integrated organization-wide risk management" [Giu+21]
"EC2"	"Defines the degree of integration between cybersecurity risk management and operational risk management" [Giu+21]	To establish whether the assessed framework "defines the degree of integration between cybersecurity risk management and operational risk management activities" [Giu+21]
"EC3"	"Clearly stating guiding principles of the framework" [Giu+21]	To determine "whether the selected framework is clearly stating its guiding principles" [Giu+21]
"EC4"	"Used for undertaking end-to-end cybersecurity risk management rather than developing cybersecurity architectures and solutions" [Giu+21]	To determine whether the assessed framework "is more relevant to undertaking end-to-end cybersecurity RM as opposed to developing architectures and solutions" [Giu+21]
"EC5"	"Relationship to standards or regulatory requirements" [Giu+21]	To establish "whether the assessed frameworks are compatible with standards or regulatory requirements" [Giu+21]
"EC6"	"Relationship to other frameworks" [Giu+21]	"To establish whether the assessed frameworks are compatible with other frameworks" [Giu+21]
"EC7"	"Risk-based rather than compliance-based" [Giu+21]	To inform whether the selected framework "aligns with a risk-based as opposed to a compliance-based approach" [Giu+21]
"EC8"	"Asset-oriented rather than threat-oriented risk analysis approach" [Giu+21]	Relates to "the nature of the approach adopted while conducting risk assessments" [Giu+21]
"EC9"	"Quantitative rather than qualitative risk assessment approach" [Giu+21]	Relates to risk measurement aspects: quantitative versus qualitative [Giu+21]

Unique ID.	Evaluation Criterion	Description
"EC10"	"Provides a comprehensive set of recommended cybersecurity controls for managing risk" [Giu+21]	To outline "whether the frameworks provide a comprehensive set of recommended cybersecurity controls" [Giu+21]
"EC11"	"Provides guidance relevant to information sharing" [Giu+21]	To outline whether the frameworks provide "guidance relevant to information sharing activities for risk management" [Giu+21]
"EC12"	"Available supporting documentation (procedures, templates, methods, case studies, etc.)" [Giu+21]	To explore "whether the assessed frameworks come together with available supporting documentation" [Giu+21]
"EC13"	"Periodically updated for continuous improvement" [Giu+21]	To explore whether the assessed frameworks "are periodically updated for continuous improvement" [Giu+21]

Further, the proposed evaluation methodology introduces the definition of the value ratings (see Table 4.2). These six linguistic values will be used to represent the resulting outcomes of the evaluation and to indicate "the extent to which the assessed framework meets a particular evaluation criterion", as illustrated in Table 4.2 [Giu+21].

Table 4.2. Definition of value ratings for evaluating the frameworks [Giu+21]

Value Rating	Definition
"True"	"A true value implies that the evaluation criterion is fully met" [Giu+21]
"Partly"	"A partly-true value means that the evaluation criterion applies to a certain extent, but it is not completely met" [Giu+21]
"Partly*"	"Partly-true values marked with an asterisk symbol * mean that, where applicable, the evaluation criterion applies both ways" [Giu+21]
"Partly**"	"Partly-true values marked with two asterisk symbols ** mean that the evaluation criterion applies subject to certain accessibility constraints" [Giu+21]
"False"	"A false value implies that the as-is criterion is not being met" [Giu+21]
"Unclear"	"An unclear value means that the corresponding value for the evaluation criterion cannot be precisely set to any of the other five values previously described as the required information is not clearly specified" [Giu+21]

Then, for rating each of the in-scope frameworks, the proposed methodology requires each evaluation criterion to be assigned the corresponding value rating. Thus, the framework ratings for each evaluation criterion result from framework analysis and are based on the defined linguistic values above [Pop20].

Furthermore, the third phase of the proposed evaluation methodology involves the comparison of the in-scope frameworks to establish the differences and similarities between them based on the framework ratings for each evaluation criterion [Pop20].

4.2. Evaluation of In-Scope Cybersecurity Risk Management Frameworks

Based on the proposed evaluation methodology introduced in Chapter 4.1 and on the information disseminated by the author through the research paper [Giu+21], this subchapter provides a critical evaluation of "several widespread cybersecurity risk management frameworks adopted by organizations to alleviate cyber risks" [Giu+21]. Thus, following the identification of in-scope frameworks phase, the in-scope frameworks for this critical evaluation are the following [Giu+21]:

1. "NIST's Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)"
2. "NIST's Unified Information Security Framework (NIST UISF)"
3. "Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)"
4. "Factor Analysis of Information Risk framework (FAIR)"
5. "Sherwood Applied Business Security Architecture (SABSA)"
6. "MITRE's Cyber Resiliency Engineering Framework (MITRE CREF)"
7. "AICPA's Cybersecurity Risk Management Reporting Framework (AICPA)"
8. "CIS Controls version 7 framework (CIS)"

Consequently, based on the information disseminated by the author through the research paper [Giu+21], Table 4.3 summarizes the findings of the evaluation for each of the selected cybersecurity risk management frameworks in relation to the above evaluation criteria introduced in Chapter 4.1 [Giu+21].

It is worthwhile noting that "when a particular framework meets a specific criterion as opposed to the other in-scope frameworks, this aspect only indicates an intrinsic property of the framework in question rather than positioning it in front of the other frameworks"; in other words, "the discrepancies highlighted between the frameworks are merely helping organizations with their decision-making process when determining the most appropriate framework to fulfill their specific needs" [Giu+21].

Table 4.3. Evaluation of selected cybersecurity risk management frameworks [Giu+21]

Unique ID.	Evaluation Criterion	NIST CSF	NIST UISF	OCTAVE	FAIR	SABSA	MITRE CREF	AICPA	CIS
"EC1"	"Integrated organization-wide risk management" [Giu+21]	True	True	False	False	True	Partly	False	False
"EC2"	"Defines the degree of integration between cybersecurity risk management and operational risk management" [Giu+21]	True	False	False	False	True	False	False	True
"EC3"	"Clearly stating guiding principles of	Partly	Partly	True	False	True	True	True	True

Unique ID.	Evaluation Criterion	NIST CSF	NIST UISF	OCTAVE	FAIR	SABSA	MITRE CREF	AICPA	CIS
	the framework” [Giu+21]								
“EC4”	“Used for undertaking end-to-end cybersecurity risk management rather than developing cybersecurity architectures and solutions” [Giu+21]	True	True	Partly	Partly	Partly*	Partly	Partly	Partly
“EC5”	“Relationship to standards or regulatory requirements” [Giu+21]	True	True	True	True	True	True	True	True
“EC6”	“Relationship to other frameworks” [Giu+21]	True	True	True	True	True	True	True	True
“EC7”	“Risk-based rather than compliance-based” [Giu+21]	True	True	True	True	True	True	False	Partly*
“EC8”	“Asset-oriented rather than threat-oriented risk analysis approach” [Giu+21]	Unclear	False	True	True	True	False	True	Partly*
“EC9”	“Quantitative rather than qualitative risk assessment approach” [Giu+21]	Unclear	False	False	True	Partly*	Unclear	Unclear	False
“EC10”	“Provides a comprehensive set of recommended cybersecurity controls for managing risk” [Giu+21]	Partly	True	True	False	True	Partly	True	True
“EC11”	“Provides guidance relevant to information sharing” [Giu+21]	True	True	False	False	True	True	True	Partly
“EC12”	“Available supporting documentation (procedures, templates, methods, case studies, etc.)” [Giu+21]	True	True	True	Partly**	Partly**	Partly	Partly	True
“EC13”	“Periodically updated for continuous improvement” [Giu+21]	True	True	Partly	True	True	True	True	True

True – “True”; Partly-True – “Partly, Partly*, Partly**”; False – “False”; Not-Clear – “Unclear”

Following Table 4.3, based on the information disseminated by the author through the research paper [Giu+21], this subchapter presents the comparison of in-scope cybersecurity risk management frameworks for each evaluation criterion [Giu+21].

"Integrated organization-wide risk management (EC1)": It is apparent from Table 4.3 that "while NIST CSF, NIST UISF, and SABSA frameworks set the scene for managing cybersecurity risk as a holistic undertaking that is fully integrated across the entire organization (i.e., integrated organization-wide risk management) [NIS18a], [NIS13], [NIS10], [NIS14], [NIS12a], [NIS11], [She+09], [She+05], OCTAVE, FAIR, MITRE CREF, AICPA and CIS frameworks are rather important enablers for the cybersecurity risk management considering that OCTAVE and FAIR frameworks are primarily focused on the risk assessment component, MITRE CREF is mainly concerned with cyber resilience, the AICPA framework is relevant to cybersecurity risk reporting, and the CIS framework's scope is limited to the risk assessment and treatment elements of the overall risk management lifecycle [SEI07], [Bod+11], [CIS18c], [CIS18b], [Fre+15]" [Giu+21]. Hence, the "EC1" is fully met by the "NIST CSF", "NIST UISF", and "SABSA" frameworks, it is met to a certain extent by the "MITRE CREF" framework, and it is not met by the "OCTAVE", "FAIR", "AICPA", and "CIS" frameworks. Moreover, "NIST CSF, NIST UISF, and SABSA frameworks are more appropriate to be considered while organizations are aiming to achieve a consistent all-encompassing approach to managing risk" [Giu+21].

"Defines the degree of integration between cybersecurity risk management and operational risk management (EC2)": "The NIST CSF clearly defines the degree of integration between cybersecurity risk management and operational risk management through the Framework Implementation Tiers (aka Tiers), SABSA framework provides the SABSA Maturity Profile (SMP) for benchmarking the maturity and integration of SABSA processes [She+09], [She+05], and the CIS framework clearly makes reference to the Tiers [NIS18a], [CIS18b]", whereas "the other selected frameworks do not specifically define the degrees of integration between cybersecurity risk management and operational risk management" [Giu+21]. Therefore, the "EC2" is fully met by "NIST CSF", "SABSA", and "CIS" frameworks and it is not met by the remaining frameworks. Moreover, "in contrast to the other in-scope frameworks, the NIST CSF, SABSA, and CIS frameworks provide means to describe the level of integration between risk management processes" [Giu+21].

"Clearly stating guiding principles of the framework (EC3)": While "the OCTAVE, SABSA, MITRE CREF, AICPA, and CIS frameworks clearly state their guiding principles [She+09], [Bod+11], [CIS18c], [Alb+01], [AIC17b]", the other frameworks "either do not provide such principles as FAIR framework or are merely making reference to such principles like NIST CSF and NIST UISF frameworks do [NIS18a], [NIS13], [NIS10], [NIS14], [NIS12a], [NIS11]" [Giu+21]. Hence, the "EC3" is fully met by the "OCTAVE", "SABSA", "MITRE CREF", "AICPA", and "CIS" frameworks, it is met to a certain extent by the "NIST CSF" and "NIST UISF" frameworks, and it is not met by the "FAIR" framework.

"Used for undertaking end-to-end cybersecurity risk management rather than developing cybersecurity architectures and solutions (EC4)": While "the SABSA framework is used both for developing cybersecurity architectures and managing cybersecurity risk [She+05]", the "NIST CSF" and "NIST UISF" frameworks "are predominantly used for holistic cybersecurity risk management [NIS18a], [NIS13], [NIS10], [NIS14], [NIS12a], [NIS11]", and the remaining frameworks (i.e., "OCTAVE", "FAIR", "MITRE CREF", "AICPA", and "CIS") "are merely partially used for undertaking cybersecurity risk management as they do not cover the entire scope of the overall cybersecurity risk management lifecycle [ISF14], [SEI07], [Bod+11], [CIS18b], [Fre+15], [AIC17b]" [Giu+21]. Thus, the "EC4" is fully met by the "NIST CSF" and "NIST UISF" frameworks, it applies both ways to the "SABSA" framework, and it is met to a certain extent by the "OCTAVE", "FAIR", "MITRE CREF", "AICPA", and "CIS" frameworks. Moreover, from the in-scope frameworks, "NIST CSF, NIST UISF, and SABSA frameworks should be considered by organizations aiming to undertake end-to-end cybersecurity risk management, and SABSA in particular is appropriate for developing cybersecurity architectures and solutions as well" [Giu+21].

"Relationship to standards or regulatory requirements (EC5), and Relationship to other frameworks (EC6)": Each of the evaluated frameworks (i.e., "NIST CSF", "NIST UISF", "OCTAVE", "FAIR", "SABSA", "MITRE CREF", "AICPA" and "CIS") "makes reference to cybersecurity and risk management frameworks and standards or regulatory requirements [NIS13], [NIS10], [SEI07], [Bod+11], [CIS18c], [AIC17b] to assist the readers with informative references [NIS18a] and normative references [The13], to support the integration with other standards and/or frameworks [She+09] or to complement other standards and/or frameworks [The13]" [Giu+21]. Thus, both "EC5" and "EC6" are fully met by all in-scope cybersecurity risk management frameworks.

"Risk-based rather than compliance-based (EC7)": With respect to this evaluation criterion, "while nearly all evaluated frameworks (i.e., NIST CSF, NIST UISF, OCTAVE, FAIR, SABSA, and MITRE CREF) follow a risk-based approach relying on risk assessments to manage cybersecurity risks, the AICPA framework follows a compliance-based approach listing a set of principles and criteria (i.e., trust services principles and criteria) for organizations to benchmark their cybersecurity against them [AIC17b], and the CIS framework can either employ a compliance-based (i.e., supported by the CIS controls) [CIS18c] or a risk-based (i.e., supported by CIS Risk Assessment Method) approach [CIS18b]" [Giu+21]. Hence, the "EC7" is fully met by the "NIST CSF", "NIST UISF", "OCTAVE", "FAIR", "SABSA", and "MITRE CREF", it applies both ways to the "CIS" framework, and it is not met by the "AICPA" framework.

"Asset-oriented rather than threat-oriented risk analysis approach (EC8)": Considering this evaluation criterion related to the risk analysis approach, "while the risk analysis pertaining to a couple of frameworks (i.e., OCTAVE, FAIR, SABSA and AICPA) is conducted by means of an asset-oriented approach which proceeds with identifying the assets in scope [SEI07], [She+05], [AIC17b], [The13]", the risk analysis processes provided along with the "NIST UISF" and "MITRE CREF" frameworks "follow a threat-oriented approach where the threat landscape is identified first [NIS12a], [Bod+11]", and the risk analysis proposed by the "CIS" framework "can be used both ways [CIS18b]" [Giu+21]. In addition, "NIST CSF" is "neither prescribing a threat-oriented nor an asset-oriented approach while undertaking risk assessments giving that it does not suggest a specific implementation order or imply a degree of importance of the Framework Core components [NIS18a]" [Giu+21]. Thus, the "EC8" is fully met by the "OCTAVE", "FAIR", "SABSA", and "AICPA" frameworks, it applies both ways to the "CIS" framework, it is not met by the "NIST UISF" framework, and it is unclear for the "NIST CSF" framework.

"Quantitative rather than qualitative risk assessment approach (EC9)": Regarding this evaluation criterion related to the risk measurement aspects, "while FAIR framework supports a quantitative assessment used to compute the risk on a quantitative scale [Fre+15], three of the evaluated frameworks (i.e., NIST UISF, OCTAVE and CIS) do not support a purely quantitative assessment [NIS12a], [SEI07], [CIS18c], the SABSA framework supports both quantitative and qualitative assessments [She+05], and the remaining three frameworks from the evaluation (i.e., NIST CSF, MITRE CREF, and AICPA) do not prescribe a particular assessment approach that is to be followed [NIS18a], [Bod+11], [AIC17b]" [Giu+21]. Thus, the "NIST UISF" framework supports "both qualitative (i.e., based on non-numerical categories or levels) [Tal+13], [Tau14], [NIS12a], [Nur+17] and semi-quantitative assessments, and provides their assessment scales as part of the appendices of NIST SP 800-30 [NIS12a]" [Giu+21]. Likewise, the "OCTAVE" framework "supports qualitative assessments rather than quantitative ones, although it may be used for simple quantitative analysis of risk [SEI07]" [Giu+21]. And, the "CIS" framework "supports both qualitative and semi-quantitative assessments as described in CIS Risk Assessment Method [CIS18b]" [Giu+21]. Thus, the "EC9" is fully met by the "FAIR" framework, it applies both ways to the "SABSA" framework, it is not met by the "NIST UISF", "OCTAVE", and "CIS" frameworks, and it is unclear for the "NIST CSF", "MITRE CREF", and "AICPA" frameworks.

"Provides a comprehensive set of recommended cybersecurity controls for managing risk (EC10)": With respect to this evaluation criterion related to cybersecurity controls, while "NIST UISF, OCTAVE, SABSA, AICPA, and CIS frameworks provide recommended security controls [NIS13], [SEI07], [CIS18c], [She+05], [AIC17b]", the other frameworks "either do not specifically address the recommended controls for cybersecurity risk mitigation as FAIR does [Fre+15] or partially address these, specifically the NIST CSF provides a set of recommended cybersecurity activities and informative references rather than a checklist of actions to perform and MITRE CREF merely provides cyber resiliency practices with key resilience-related activities as it is principally focused on the resilience component of the cybersecurity [NIS18a], [Bod+11]" [Giu+21]. Thus, the "EC10" is fully met by the "NIST UISF", "OCTAVE", "SABSA", "AICPA", and "CIS" frameworks, it is met to a certain extent by the "NIST CSF" and "MITRE CREF" frameworks, and it is not met by the "FAIR" framework. Moreover, from the in-scope frameworks, "organizations should consider referring to the NIST UISF, OCTAVE, SABSA, AICPA, and CIS frameworks when looking for comprehensive sets of recommended controls to specifically address cybersecurity risk" [Giu+21].

"Provides guidance relevant to information sharing (EC11)": "The NIST CSF, NIST UISF, SABSA, MITRE CREF, and AICPA frameworks provide guidance relevant to information sharing and situational awareness for organizations to consider while strengthening their cybersecurity programmes [NIS18a], [NIS13], [NIS10], [NIS14], [NIS12a], [NIS11], [Bod+11], [She+05], [AIC17b]", whereas "other frameworks either do not provide this level of guidance like OCTAVE and FAIR do [SEI07], [Fre+15] or only scratch the surface by referencing other related documentation as the CIS framework does [CIS18c]" [Giu+21]. Hence, the "EC11" is fully met by the "NIST CSF", "NIST UISF", "SABSA", "MITRE CREF", and "AICPA" frameworks, it is met to a certain extent by the "CIS" framework, and it is not met by the "OCTAVE" and "FAIR" frameworks.

"Available supporting documentation (procedures, templates, methods, case studies, etc.) (EC12), and Periodically updated for continuous improvement (EC13)": "The NIST CSF, NIST UISF, OCTAVE, and CIS frameworks provide supporting documentation which is freely available [NIS18a], [NIS13], [NIS10], [NIS14], [NIS12a], [NIS11], [SEI07], [CIS18c]", whereas "the remaining in-scope frameworks either do not make the entire supporting documentation freely available as FAIR and SABSA do or the supporting documentation available could be considered rather limited than all-encompassing as in the case of the MITRE CREF and AICPA frameworks" [Giu+21]. Also, with respect to the last evaluation criterion, it is worth noting that "almost every in-scope framework is undergoing periodical updates, where OCTAVE makes exception" [Giu+21]. Thus, about the "EC12", this is fully met by the "NIST CSF", "NIST UISF", "OCTAVE", and "CIS" frameworks, it applies to the "FAIR" and "SABSA" frameworks subject to certain accessibility constraints, and it is met to a certain extent by the "MITRE CREF" and "AICPA" frameworks. As for the "EC13", this is fully met by all in-scope cybersecurity risk management frameworks, except the "OCTAVE" framework which meets "EC13" to a certain extent.

4.3. Related Work

Based on the information disseminated by the author through the PhD report [Pop20], this subchapter encompasses the related work relevant to the evaluation of in-scope cybersecurity risk management frameworks.

To provide the evaluation of in-scope cybersecurity risk management frameworks, the available documentation around the in-scope cybersecurity risk management frameworks was used. In addition, the available supporting documentation for the in-scope frameworks was even selected as an evaluation criterion (i.e., "EC12") (see Chapter 4.1) [Pop20].

Furthermore, the identification of in-scope frameworks is based on the selection criteria of choosing the frameworks that are free of charge with readily available documentation from the frameworks outlined in Chapter 2.3, which provided an overview of several widely used frameworks pertaining to three categories relevant to cybersecurity risk management which can be leveraged by any organization regardless of type, size, sector, or focus area. A similar idea of using two selection iterations was done by Kiran et al. (2013) [Kir+13] to select three information security risk assessment models for undertaking a comparative analysis between them.

Moreover, with respect to frameworks evaluation, Table 4.4 shows the related work mapped against the scope of previous research works and the approach adopted by these works to address the scope.

Table 4.4 Related work mapped against the scope and approach of previous research works [Pop20]

		How is the Scope Addressed?			
What is the Scope?		**Outlining Strengths and Weaknesses**	**Comparison Based on the Structure of the Risk Assessment / Risk Management Process**	**Comparison Based on Defined Evaluation Criteria**	**Feature-by-Feature Comparison**
"A Narrower Scope"	**"Fewer Frameworks Being Addressed"**	[Chm+14]	n/a*	n/a*	n/a*
	"Limited to a Specific Focus Area"	[Inn10]	n/a*	n/a*	[Inn10] [Gas+17] [Gje+11]
"A Partly Different Scope"	**"Addressing Best-Practices Irrespective of Types"**	[Tal+13]	[Mes+17]	[Nur+17]	[Tal+13] [Alm+17]
	"Merely-Focusing on Risk Assessment / Risk Management Methodologies / Methods"	[Ion13]	[Gha+14] [ISO09]	[Sha+16a] [Kir+13] [Lab+06] [Ion13]	[Ion13] [Rod14] [Ful17]

*Note, n/a indicates that no study was found to fit the categories at the time of this study

With respect to the scope of previous research works, related works have primarily concentrated on evaluations with a narrower scope (i.e., fewer frameworks being addressed, limited to a specific focus area) (see Chapter 4.3.1) or on evaluations with a partly different scope (i.e., addressing best-practices irrespective of types, merely-focusing on risk assessment / risk management methodologies / methods) (see Chapter 4.3.2). Also, with respect to the approach adopted by related works to address the scope, four types of approach were identified. These types include outlining strenghts and weaknesses, comparison based on the structure of the risk assessment / risk management process, comparison based on defined evaluation criteria, and feature-by-feature comparison.

As shown in Table 4.4, previous studies on evaluating cybersecurity risk management frameworks have not dealt with critical evaluations having bigger scope and have not centered their evaluations exclusively on frameworks.

4.3.1. Related Evaluation Studies With a Narrower Scope

The related works about frameworks evaluation with a narrower scope can be classified into two types [Pop20]: research studies with fewer frameworks being addressed (i.e. [Chm+14]) and research studies limited to a specific focus area of frameworks (i.e. [Inn10], [Gje+11], [Gas+17]).

As per Table 4.4, no research has been found with fewer frameworks being addressed nor has research limited to a specific area of focus been found to provide comparison based on the structure of the risk assessment / risk management process or to provide comparison based on defined evaluation criteria. Also, no research has been found to match the type of a narrower scope with fewer frameworks being addressed to provide feature-by-feature comparison [Pop20].

Further, Chmielecki et al. (2014) [Chm+14] provided a comparison of four IT risk management frameworks based on advantages and disadvantages. Regarding the studies limited to a specific focus area of frameworks, Innotrain IT (2010) [Inn10] provided an evaluation of the strenghts and weaknesses of a few frameworks (e.g., "COBIT", "ITIL") related and relevant for "Information Technology Service Management (ITSM)" along with a feature-by-feature comparison through the intersections of some of these frameworks with other frameworks, while Gjerdrum and Peter (2011) [Gje+11] and Gashgari, Walters and Wills (2017) [Gas+17] provided their evaluation only through feature-by-feature comparison. In this context, Gashgari, Walters and Wills (2017) [Gas+17] targeted the proposal of an information security governance framework based on the principles of "ISO/IEC 27014" and "COBIT". And, Gjerdrum and Peter (2011) [Gje+11] provided the comparison of scope, a few key definitions (i.e., risk management, risk, risk appetite, risk assessment) and risk management process to illustrate key differences between two generic risk management frameworks (i.e., "ISO 31000" and "COSO Enterprise Risk Management (ERM) framework") [Pop20].

In contrast to these existing works (i.e., [Chm+14], [Inn10], [Gas+17], [Gje+11]), the critical evaluation from this chapter addresses eight cybersecurity risk management frameworks and is not limiting the evaluation neither to strengths and weaknesses, nor to a feature-by-feature comparison of frameworks. Instead, the critical evaluation from this chapter is based on the proposed methodology (see Chapter 4.1) that relies on the defined evaluation criteria. Even though the proposed methodology from this chapter is much wider in scope than the study conducted by Gjerdrum and Peter (2011) [Gje+11], similar to Gjerdrum and Peter (2011) [Gje+11] who provided the comparison of scope and a few definitions of key terms between two frameworks, three of the evaluation criteria (i.e., "EC1", "EC2", "EC3") and an evaluation criterion (i.e., "EC4") of the proposed evaluation methodology from this chapter are based on the definition and purpose of the cybersecurity risk management framework to indicate the similarities and differences between the in-scope frameworks (see Fig. 4.2) [Pop20].

In addition, compared with the study performed by Innotrain IT (2010) [Inn10] who conducted a feature-by-feature comparison through the intersection of "ITSM" frameworks with other frameworks, the proposed evaluation methodology from this chapter aims to establish the compatibility of in-scope frameworks with other frameworks and standards or regulatory requirements by formulating two evaluation criteria (i.e., "EC5", "EC6"). A similar idea was introduced by ENISA (2006) [ENI06] as part of their inventory, which examined the regulatory compliance and compliance to IT standards for risk management / assessment methods [Pop20].

While formulating the evaluation criteria is an essential step for addressing "Multiple Attribute Decision Making (MADM)" problems [Tze+11], the proposed evaluation methodology was not crafted as a means of selecting one of the in-scope frameworks as a better alternative over the others. Instead, the proposed evaluation criteria were established to allow a greater characterization of frameworks through the

13 evaluation criteria belonging to the 7 dimensions of the proposed hierarchical structure for evaluating the in-scope frameworks (see Chapter 4.1). The "MADM" studies provided the basis for the proposal of the hierarchical structure of evaluation criteria used in the proposed evaluation methodology [Pop20].

4.3.2. Related Evaluation Studies With a Partly Different Scope

There have been several related evaluation studies with a partly different scope than the scope of the evaluation methodology proposed in this chapter for evaluating in-scope cybersecurity risk management frameworks [Pop20]. These studies can be classified into two types based on their scope [Pop20]: research studies addressing best-practices irrespective of types and research studies merely-focusing on the risk assessment / risk management related methodologies / methods. With respect to the research studies addressing best practices irrespective of types [Pop20], these were carried out by Talabis and Martin (2013) [Tal+13], Meszaros and Buchalcevova (2017) [Mes+17], Ghazouani et al. (2014) [Gha+14], Nurse et al. (2017) [Nur+17], and Almuhammadi and Alsaleh (2017) [Alm+17]. And, with respect to the research studies merely-focusing on the risk assessment / risk management related methodologies / methods [Pop20], these were done by Ionita (2013) [Ion13], ISO (2009) [ISO09], Shameli-Sendi, Aghababaei-Barzegar, and Cheriet, (2016a) [Sha+16a], Kiran et al. (2013) [Kir+13], Fulford (2017) [Ful17], Labuschagne and Bornman (2006) [Lab+06] and Rodion (2014) [Rod14].

Further, Table 4.4 shows that a number of related studies with a partly different scope involved evaluations based on one of these two approaches: comparison based on the structure of the risk assessment / risk management process and comparison based on defined evaluation criteria. For instance, three related research studies made their comparison based on the structure of a risk assessment / risk management process: Meszaros and Buchalcevova (2017) [Mes+17] briefly evaluated the "CORAS" and "OCTAVE Allegro" methods, the "Harmonized Threat and Risk Assessment (HTRA)" methodology, the "ISO/IEC 27005" standard, and the "NIST Risk Management Framework" by focusing on risk management; Ghazouani et al. (2014) [Gha+14] provided a comparative analysis of a few risk management methodologies based on the information security risk management process; and ISO (2009) [ISO09] compared the risk assessment techniques by describing for each step of the risk assessment process the application of the risk assessment methods as being either strongly applicable, applicable or not applicable. Similar to these three related research studies (i.e., [Mes+17], [Gha+14], [ISO09]), four evaluation criteria (i.e., "EC8", "EC9", "EC10", "EC11") of the proposed evaluation methodology from this chapter are based on the key elements pertaining to the risk management process from the hierarchical structure for evaluating the in-scope frameworks (see Fig. 4.2). Nevertheless, to allow a more comprehensive characterization of the in-scope frameworks, the critical evaluation from this chapter involves 13 evaluation criteria in total based on 7 dimensions. Moreover, same as ISO (2009) [ISO09], the resulting outcomes of the critical evaluation provided in this chapter were represented using linguistic values. However, compared with the evaluation of the risk assessment techniques provided by ISO (2009) [ISO09] where three value ratings (i.e., strongly applicable, applicable or not applicable) were used to indicate the applicability of the risk assessment methods to the steps of the risk assessment process, the critical evaluation of in-scope frameworks presented in this chapter leverages six value ratings that allows it to indicate more precisely the extent to which the assessed framework meets a particular evaluation criterion. This is also because some of the defined evaluation criteria from this chapter are more complex (e.g., "EC4", "EC7", "EC8", "EC9") to provide a more realistic analysis. For example, a similar way of expressing an evaluation criterion was done by Ionita (2013) [Ion13], who was using "quantitative or qualitative" as one of the main characteristics of the reviewed risk assessment / risk management methods. This relates to the evaluation criterion "EC9" (i.e., "Quantitative rather than qualitative risk assessment approach") presented in this chapter [Pop20].

Furthermore, several studies performed their comparisons based on defined evaluation criteria. For example, the research study conducted by Nurse et al. (2017) [Nur+17] provides a brief comparison of selected sub-processes of "NIST SP 800-30", "ISO/IEC 27001" and "OCTAVE" in terms of modus operandi (i.e., the nature of the risk assessment approach, and how risk is measured). Likewise, the evaluation criterion "EC8" (i.e., "Asset-oriented rather than threat-oriented risk analysis approach") and the evaluation criterion "EC9" (i.e., "Quantitative rather than qualitative risk assessment approach") from this chapter are formulated to address both the aforementioned aspects analyzed by Nurse et al. (2017) [Nur+17]. Similar comparison based on defined evaluation criteria was conducted by Shameli-Sendi, Aghababaei-Barzegar, and Cheriet, (2016a) [Sha+16a] who provided a comparison of information security risk assessment approaches based on a proposed taxonomy that includes four categories: appraisement, perspective, resource valuation and risk management. This research study carried out by Shameli-Sendi, Aghababaei-Barzegar, and Cheriet, (2016a) [Sha+16a] evaluated the nature of the risk assessment approach using the "perspective" term and the type of the risk measurement techniques using the "appraisement" term. Also, Kiran et al. (2013) [Kir+13] performed a comparative analysis on three information security risk assessment models based on three comparison criteria (i.e., "concept definition", "approach to information security assessment", "results and output"), in which the "results and output" criterion bears a close resemblance with two of the proposed evaluation criteria from this chapter (i.e., "EC7", "EC9"). The evaluation criterion "EC7" was extracted from the overview of the most widely adopted cybersecurity-related frameworks provided in Chapter 2.3. Moreover, Labuschagne and Bornman (2006) [Lab+06] used the "COBIT's Planning and Organization Control Nine", "Assess Risks" as evaluation criteria, to provide a comparative framework for evaluating information security risk management methods [Pop20].

Regarding the studies with a partly different scope outlining strengths and weaknesses, Talabis and Martin (2013) [Tal+13] outlined the strenghts and weaknesses of some major information security risk assessment frameworks (i.e., "OCTAVE", "FAIR", "NIST SP 800-30") and of the information security risk management standard "ISO 27005", and Ionita (2013) [Ion13] provided the pros and cons while evaluating the information security risk management / risk assessment methods [Pop20].

Moreover, five research studies with a partly different scope providing feature-by-feature comparison were reviewed. In this sense, Talabis and Martin (2013) [Tal+13] provided a comparison of the major activities for three frameworks and a standard. Almuhammadi and Alsaleh (2017) [Alm+17] compared "NIST CSF" framework to "COBIT" framework, "ISO / IEC 27001" standard, and "ISF Standard of Good Practice for Information Security". Also, Ionita (2013) [Ion13] evaluated the naming variations between information security conceptual models of risk rating methodologies. In addition, Rodion (2014) [Rod14] compared the structure of the guides belonging to two information security risk assessment methods. And, Fulford

(2017) [Ful17] identified the differences between academic and practitioner technology risk management methodologies by evaluating the type of technology risk model, the primary technology risk measurement technique, the technology risk measurement process, the primary technology risk focus, the primary security domain assessed and the organizational implementation. Again, the evaluation criterion "EC9" proposed in this chapter bears a close resemblance [Pop20] with the type of technology risk model criteria used by Fulford (2017) [Ful17].

4.4. Conclusions

This chapter extended the research work on the cybersecurity risk management frameworks outlined in Chapter 2 by proposing a methodology for evaluating cybersecurity risk management frameworks, critically evaluating the in-scope cybersecurity risk management frameworks and providing a comprehensive analysis of the related work. Thus, this chapter aimed to support decision-making when it comes to cybersecurity risk management framework selection and to facilitate pragmatic implementation of cybersecurity programmes by addressing the need for more evaluations of these frameworks relative to each other.

First, this chapter provided the design of the three-phased methodology that was proposed for evaluating the in-scope cybersecurity risk management frameworks. With respect to the first phase of the methodology, namely the "identification of in-scope frameworks" phase, this makes use of the overview of the cybersecurity risk management frameworks and the selection criteria of choosing only free of charge frameworks with readily available documentation to determine the in-scope frameworks. Thus, to identify the in-scope frameworks, the selection criteria is applied to the cybersecurity risk management frameworks described in the overview from Chapter 2.3. Then, with respect to the second phase of the methodology, namely the "analysis of in-scope frameworks" phase, this makes use of a proposed hierarchical structure for evaluating frameworks based on "Multiple Attribute Decision Making (MADM)" approach and the definition of the value ratings to analyse the in-scope cybersecurity risk management frameworks and to determine the framework ratings. With respect to the proposed hierarchical structure, it consists of seven dimensions and thirteen evaluation criteria, where these criteria were formulated to allow a greater characterization of frameworks based on the following dimensions: the definition, purpose, and type of the cybersecurity risk management framework, compatibility with other frameworks and standards or regulatory requirements, key elements pertaining to the risk management process, available supporting documentation, and continuous framework improvement. As for the definition of the value ratings, six linguistic values were defined. Thus, to determine the framework ratings, the analysis of the in-scope frameworks involved assigning linguistic value ratings to each of the evaluation criteria for each of the in-scope frameworks to indicate the extent to which in-scope frameworks meet specific evaluation criteria. Furthermore, with respect to the third phase of the methodology, namely the "comparison of in-scope frameworks" phase, this makes use of the framework ratings resulted from the second phase of the proposed methodology to establish the differences and similarities between the in-scope cybersecurity risk management frameworks.

Second, this chapter provided the critical evaluation of the in-scope cybersecurity risk management frameworks. Hence, there were eight cybersecurity risk management frameworks identified as in scope, namely the "NIST's Framework for Improving Critical Infrastructure Cybersecurity", "NIST's Unified Information

Security Framework", "Operationally Critical Threat, Asset, and Vulnerability Evaluation", "Factor Analysis of Information Risk framework", "Sherwood Applied Business Security Architecture", "MITRE's Cyber Resiliency Engineering Framework", "AICPA's Cybersecurity Risk Management Reporting Framework", and "CIS Controls version 7" framework. Furthermore, the critical evaluation of these frameworks was outlined together with the findings which offer a consolidated characterization of the in-scope cybersecurity risk management frameworks and emphasize similarities and differences between them through the thirteen evaluation criteria of the proposed evaluation methodology.

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

This chapter provided the following contributions:

- The design of a three-phased methodology that involves identification, analysis, and comparison of in-scope cybersecurity risk management frameworks;
- The development of a hierarchical structure for evaluating the in-scope cybersecurity risk management frameworks, which includes seven dimensions and thirteen evaluation criteria;
- The definition of six linguistic values for rating the in-scope cybersecurity risk management frameworks against the evaluation criteria;
- The critical evaluation of eight cybersecurity risk management frameworks based on the proposed evaluation methodology;
- A comprehensive analysis of the related work relevant to the evaluation of cybersecurity risk management frameworks that delved into previous studies with a narrower scope and a partly different scope.

5. IoT SECURITY RISK MANAGEMENT STRATEGY REFERENCE MODEL (IoTSRM2)

Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], this chapter builds on the overview of IoT security best practices provided in Chapter 2.4. Thus, given "the prevalent absence of robust IoT security risk management strategies in organizations [Lee20], [McK17] coupled with the paucity of IoT security risk management strategy reference sources [Lee20], [WEF20a]", this chapter aims to address "the research gap in terms of the existence of an IoT security risk management strategy reference model" [Pop+21a]. Hence, the purpose of this chapter 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" [Pop+21a]. 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" [Pop+21a].

First, the chapter describes "the three-phased methodology for developing the proposed IoT security risk management strategy reference model (IoTSRM2)" [Pop+21a]. Then, the chapter 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" [Pop+21a]. Further, the chapter provides "the critical evaluation of selected informative references of IoTSRM2" [Pop+21a]. Finally, the chapter outlines the related work by critically evaluating the IoTSRM2 and 25 selected IoT security best practices using eight evaluation criteria.

Thus, this chapter addresses the following thesis objective:

- **Objective 8:** Propose a methodology for developing a reference model for IoT security risk management strategy, propose the IoT security risk management strategy reference model (IoTSRM2), and evaluate the proposed IoTSRM2 against the IoT security best practices that are the most relevant for the proposed model.

5.1. Proposed Methodology for Developing the IoTSRM2

Based on the information disseminated by the author through the research paper [Pop+21a], this subchapter describes "the methodology used for developing the proposed IoT Security Risk Management Strategy Reference Model (IoTSRM2)" [Pop+21a]. Fig. 5.1 shows "the 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)" [Pop+21a].

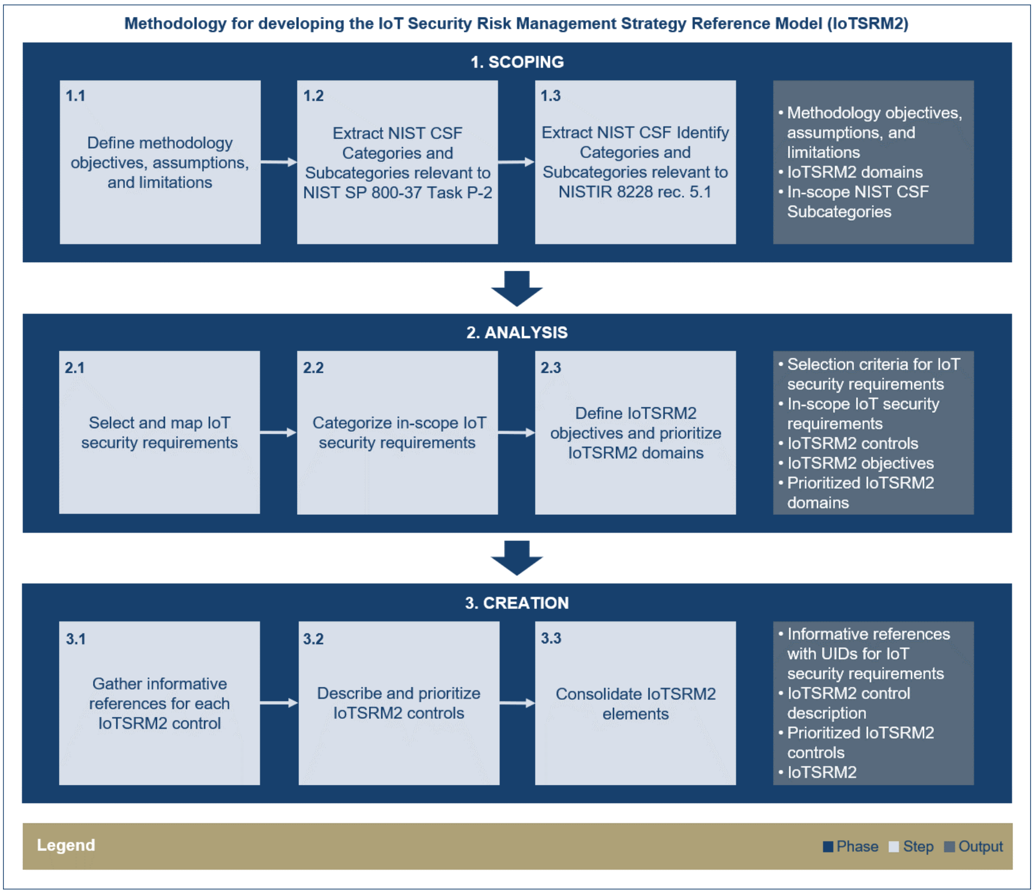

Methodology for developing the IoT Security Risk Management Strategy Reference Model (IoTSRM2)
1. SCOPING
1.1
Define methodology objectives, assumptions, and limitations
1.2
Extract NIST CSF Categories and Subcategories relevant to NIST SP 800-37 Task P-2
1.3
Extract NIST CSF Identify Categories and 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

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

Further, based on the information disseminated by the author through the research paper [Pop+21a], each of the three phases of the proposed methodology together with its corresponding steps are described below [Pop+21a].

5.1.1. Phase 1: Scoping

Based on the information disseminated by the author through the research paper [Pop+21a], 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)" [Pop+21a].

"Step 1.1": "Define methodology objectives, assumptions, and limitations"

First, this step outlines "the ten objectives of the proposed methodology" [Pop+21a]. Thus, based on the information disseminated by the author through the research paper [Pop+21a], the main objectives of the proposed methodology are [Pop+21a]:

- **"Objective 5.1"**: "Develop a reference model for IoT security risk management strategy applicable to IoT adopters from any sector" [Pop+21a];
- **"Objective 5.2"**: "Develop the proposed reference model based on NIST CSF [NIS18a] and selected IoT security best practices" [Pop+21a] (see Chapter 2.4).

Then, based on the information disseminated by the author through the research paper [Pop+21a], "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. (2017) [Mai+17]" [Pop+21a].

"In terms of the structural granularity dimension", the objective of the proposed methodology is [Pop+21a]:

- **"Objective 5.3"**: "Organize the proposed reference model in hierarchical structures, including domain level, objective level, and control level" [Pop+21a].

"As for the information granularity dimension", the objectives of the proposed methodology are [Pop+21a]:

- **"Objective 5.4"**: "Identify IoT security domains to group IoT security objectives for the proposed reference model" [Pop+21a];
- **"Objective 5.5"**: "Define high-level IoT security objectives to group IoT security controls for the proposed reference model" [Pop+21a];
- **"Objective 5.6"**: "Define the criteria for selecting IoT security requirements from selected IoT security best practices" [Pop+21a];
- **"Objective 5.7"**: "Define IoT security controls for the proposed IoT security objectives based on selected IoT security requirements from the in-scope IoT security best practices" [Pop+21a];
- **"Objective 5.8"**: "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" [Pop+21a];
- **"Objective 5.9"**: "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" [Pop+21a];
- **"Objective 5.10"**: "Provide the prioritization rating for each of the proposed IoT security controls" [Pop+21a].

Furthermore, this step provides "the assumptions on which the proposed methodology is based" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a], 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 [NIS18a]" [Pop+21a];
- "IoT adopters are assumed to outsource IoT software development and not engage in in-house IoT software development activities" [Pop+21a];

- "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" [Pop+21a].

In addition, "Step 1.1" provides "the limitations of the proposed methodology" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a], these limitations are enumerated below:

- "The proposed methodology is derived, based on, and limited to expert judgement and selected best practices" [Pop+21a];
- "The proposed methodology is limited to the assumptions on which it is based" [Pop+21a].

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

Based on the information disseminated by the author through the research paper [Pop+21a], "Step 1.2" funnels "NIST CSF Core to focus the proposed reference model on those Categories and Subcategories that are more relevant to Risk Management Strategy" [Pop+21a]. 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 [NIS18b]" [Pop+21a].

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

Based on the information disseminated by the author through the research paper [Pop+21a], "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" [Pop+21a]. 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 [NIS19b]" [Pop+21a]. Hence, "it allows the determination of the domains for the IoTSRM2 and the in-scope NIST CSF Subcategories for the IoTSRM2 objectives" [Pop+21a]. Further, the "IoTSRM2" domains are represented using the Equation (5.1) where "x_i represents the six domains of IoTSRM2, and C represents the cardinality of x_i" [Pop+21a]:

$$x_i = \left\{ \begin{array}{c} \text{"Asset Management", "Business Environment", "Governance",} \\ \text{"Risk Assessment", "Risk Management Strategy",} \\ \text{"Supply Chain Risk Management"} \end{array} \right\}, \tag{5.1}$$

$$\text{where } C = |x_i| = 6,\ i = [1..C]$$

5.1.2. Phase 2: Analysis

Then, based on the information disseminated by the author through the research paper [Pop+21a], 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)" [Pop+21a].

"Step 2.1": "Select and map IoT security requirements"

Based on the information disseminated by the author through the research paper [Pop+21a], this step involves "the identification of the in-scope IoT security requirements from 25 selected IoT security best practices" [Pop+21a] (see Chapter 2.4). First, IoT security requirements are selected by "applying on the selected IoT security best practices the selection criteria outlined below" [Pop+21a]:

- **"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" [Pop+21a];
- **"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/maintainance and/or disposal of IoT devices and/or services for IoT adopters" [Pop+21a];
- **"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/maintainance and/or disposal of IoT devices and/or services for IoT adopters" [Pop+21a].

Then, the resulting IoT security requirements "are analysed relative to the in-scope NIST CSF Subcategories from Step 1.3 to determine the in-scope IoT security requirements" [Pop+21a]. Hence, the IoT security requirements "are mapped against the in-scope NIST CSF Subcategories from Step 1.3" [Pop+21a].

"Step 2.2": "Categorize in-scope IoT security requirements"

Based on the information disseminated by the author through the research paper [Pop+21a], "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" [Pop+21a]. 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" [Pop+21a]. 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" [Pop+21a]. These groups allow "the naming of IoTSRM2 controls" (see Chapter 5.2) [Pop+21a].

"Step 2.3": "Define IoTSRM2 objectives and prioritize IoTSRM2 domains"

Based on the information disseminated by the author through the research paper [Pop+21a], 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" [Pop+21a]. 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" [Pop+21a] (see Chapter 5.2). The "IoTSRM2" objectives are represented using the Equations from (5.2) to (5.7) [Pop+21a]:

- "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" [Pop+21a]:

$$x_{1j}=\left\{\begin{matrix}\text{"Hardware inventory",}\\ \text{"Software inventory"}\end{matrix}\right\}, \quad \text{where } C_1=|x_{1j}|=2,\ j=[1..C_1],\ n_{1j}=\{1,1\} \tag{5.2}$$

- "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" [Pop+21a]:

$$x_{2j}=\left\{\begin{matrix}\text{"Dependencies and critical functions",}\\ \text{"Critical service resilience"}\end{matrix}\right\}, \quad \text{where } C_2=|x_{2j}|=2,\ j=[1..C_2],\ n_{2j}=\{1,1\} \tag{5.3}$$

- "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" [Pop+21a]:

$$x_{3j}=\left\{\begin{matrix}\text{"Security related policies",}\\ \text{"Structures and responsibilities",}\\ \text{"Regulatory requirements",}\\ \text{"Governance and risk management plans"}\end{matrix}\right\}, \quad \text{where } C_3=|x_{3j}|=4,\ j=[1..C_3],\ n_{3j}=\{4,2,1,7\} \tag{5.4}$$

- "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" [Pop+21a]:

$$x_{4j}=\left\{\begin{matrix}\text{"Vulnerability discovery",}\\ \text{"Threat identification",}\\ \text{"Risk analysis",}\\ \text{"Risk responses"}\end{matrix}\right\}, \quad \text{where } C_4=|x_{4j}|=4,\ j=[1..C_4],\ n_{4j}=\{2,2,1,1\} \tag{5.5}$$

- "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" [Pop+21a]:

$$x_{5j}=\left\{\begin{matrix}\text{"Risk appetite and tolerances",}\\ \text{"Context-informed risk tolerances"}\end{matrix}\right\}, \tag{5.6}$$

$$\text{where } C_5=|x_{5j}|=2,\ j=[1..C_5],\ n_{5j}=\{1,1\}$$

- "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" [Pop+21a]:

$$x_{6j}=\left\{\begin{array}{c}\text{"Supplier assessment",}\\ \text{"Supplier contract management"}\end{array}\right\}, \qquad \text{where } C_6=|x_{6j}|=2,\ j=[1..C_6],\ n_{6j}=\{2,2\} \tag{5.7}$$

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" [Pop+21a]. Thus, based on the information disseminated by the author through the research paper [Pop+21a], Equation (5.8) provides "the weight of each IoTSRM2 objective" [Pop+21a]:

$$\text{Weight } (x_{ij}) = \frac{1}{\sum_1^C C_q}, \text{ where } i=[1..C],\ j=[1..C_i], \sum_1^{\sum_1^C C_q} \frac{1}{\sum_1^C C_q}=100\% \tag{5.8}$$

Then, based on the information disseminated by the author through the research paper [Pop+21a], the "IoTSRM2" domains are prioritized using the following formula [Pop+21a]:

$$\text{Weight } (x_i) = \frac{C_i}{\sum_1^C C_q}, \text{ where } i=[1..C], \sum_{i=1}^{C} \frac{C_i}{\sum_1^C C_q}=100\% \tag{5.9}$$

5.1.3. Phase 3: Creation

Then, based on the information disseminated by the author through the research paper [Pop+21a], 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)" [Pop+21a].

"Step 3.1": "Gather informative references for each IoTSRM2 control"

For each "IoTSRM2" control, based on the information disseminated by the author through the research paper [Pop+21a], 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" [Pop+21a] (see Chapter 5.2). 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" [Pop+21a]. Notwithstanding, "the sole implementation of the IoT security requirements from the informative references does not necessarily lead to IoTSRM2 compliance" [Pop+21a].

"Step 3.2": "Describe and prioritize IoTSRM2 controls"

Based on the information disseminated by the author through the research paper [Pop+21a], 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" [Pop+21a] (see Chapter 5.2). Then, the "IoTSRM2" controls "are prioritized for each IoTSRM2 objective based on their corresponding adjusted weights" which are determined using Equations (5.10 and 5.11) [Pop+21a].

Equation (5.10) allows "the determination of the IoTSRM2 control weights" [Pop+21a]. 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" [Pop+21a]. In this equation, "x_{ijk} represents the controls of the x_{ij} objectives of the x_i domains of IoTSRM2, $R(x_{ijk})$ represents the number of in-scope IoT security requirements applicable for each of the x_{ijk} controls of each of the x_{ij} objectives of each of the x_i domains of IoTSRM2, $I(x_{ijk})$ represents the number of informative references applicable for each of the x_{ijk} controls of each of the x_{ij} objectives of each of the x_i domains of IoTSRM2, and p represents the number of selected IoT security best practices" [Pop+21a] (see Chapter 2.4).

$$\text{Weight }(x_{ijk}) = \frac{R(x_{ijk})}{I(x_{ijk})} + \frac{R(x_{ijk})}{p} \ , \quad \text{where } i=[1..C],\ j=[1..C_i],\ k=[1..n_{ij}] \tag{5.10}$$

Then the resulting control weights "are adjusted using Equation (5.11) to ensure normalization of values so that the weights of the IoTSRM2 controls of any IoTSRM2 objective add up to 100%" [Pop+21a].

$$\text{Adjusted weight }(x_{ijk}) = \frac{1}{\sum_1^C C_q} * \frac{\text{Weight }(x_{ijk})}{\sum_{s=1}^{n_{ij}} \text{Weight }(x_{ijs})} * 100\% \ , \quad \text{where } i=[1..C],\ j=[1..C_i],\ k=[1..n_{ij}], \sum_{i=1}^{C}\sum_{j=1}^{C_i}\sum_{k=1}^{n_{ij}} \text{Adjusted weight }(x_{ijk})=100\% \tag{5.11}$$

"Step 3.3": "Consolidate IoTSRM2 elements"

To showcase the proposed "IoTSRM2" (see Chapter 5.2), based on the information disseminated by the author through the research paper [Pop+21a], "Step 3.3 brings together the following IoTSRM2 elements, not necessarily in that order":

- "IoTSRM2 domains, objectives, and controls" [Pop+21a];

- "for each IoTSRM2 control, applicable informative references with associated unique identifiers of the in-scope IoT security requirements" [Pop+21a];
- "for each IoTSRM2 objective, the prioritization of IoTSRM2 controls based on their corresponding adjusted weights" [Pop+21a];
- "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" [Pop+21a].

Note, based on the information disseminated by the author through the research paper [Pop+21a], "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" [Pop+21a]:

- **"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" [Pop+21a];
- **"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" [Pop+21a];
- **"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" [Pop+21a];
- **"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" [Pop+21a].

5.2. The Proposed IoTSRM2

Based on the 25 selected IoT security best practices outlined in Chapter 2.4 and on the methodology introduced in Chapter 5.1, this subchapter provides "the proposed IoT security risk management strategy reference model (IoTSRM2) which bridges one major research gap in IoT security risk management strategy, namely the absence of a reference model for IoT security risk management strategy" [Pop+21a]. First, based on the information disseminated by the author through the research paper [Pop+21a], Fig. 5.2 "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" [Pop+21a]. As depicted in Fig. 5.2, "the proposed IoTSRM2 consists of six domains, sixteen objectives, and thirty controls" [Pop+21a]. 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" [Pop+21a]. 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" [Pop+21a].

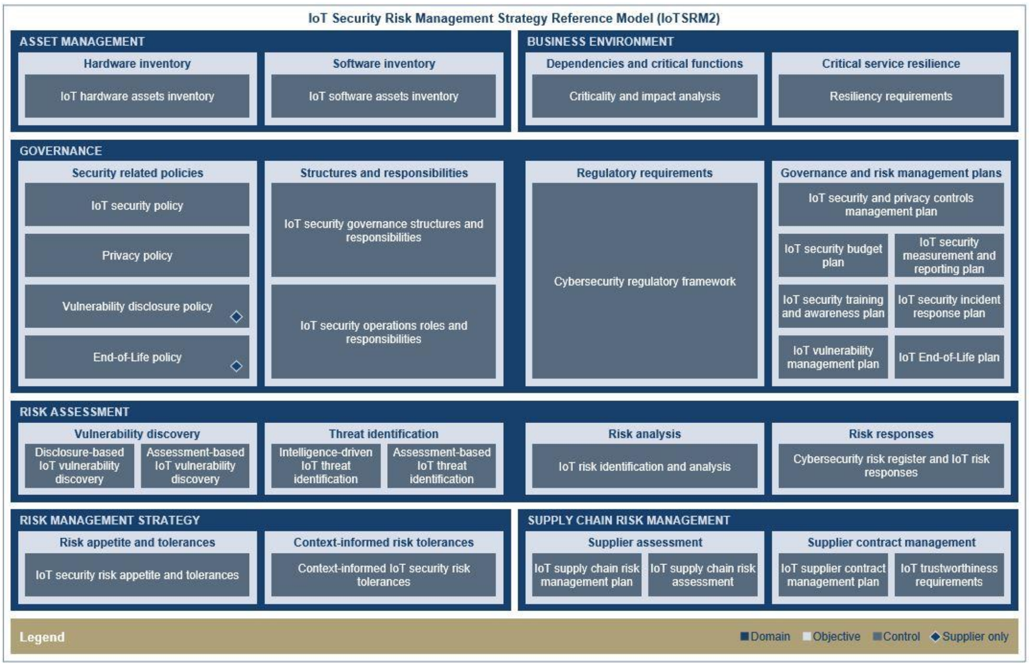

IoT Security Risk Management Strategy Reference Model (IoTSRM2)
ASSET MANAGEMENT
Hardware inventory
IoT hardware assets inventory
Software inventory
IoT software assets inventory
BUSINESS ENVIRONMENT
Dependencies and critical functions
Criticality and impact analysis
Critical service resilience
Resiliency 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

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

Then, Table 5.1 shows, in descending order, the total number of unique IoT security requirements mapped against the "IoTSRM2" of each informative reference, and it indicates those informative references that classify among the informative references that are considered the most relevant to IoT security risk management strategy [Pop+21a], [Pop21]. As per Table 5.1, seven informative references resulted "the most relevant to IoT security risk management strategy as they meet the two inclusion criteria and two conditions from Step 3.3 of the proposed methodology" outlined in Chapter 5.1 [Pop+21a].

Table 5.1. Total number of unique IoT security requirements mapped. Adapted from [Pop+21a]

Informative Reference	**Name of Informative Reference**	**Total # of Unique in-Scope IoT Security Requirements Mapped**
[ENI18b]*	"ENISA's Good Practices for Security of Internet of Things in the context of Smart Manufacturing*"	"54"
[CSA19a]*	"CSA IoT Security Controls Framework Version 1"	"41"

Informative Reference	Name of Informative Reference	Total # of Unique in-Scope IoT Security Requirements Mapped
[IoT20a]*	“IoTSF’s IoT Security Compliance Framework Release 2.1”	“34”
[Age20a]*	“AgeLight’s IoT Safety Architecture & Risk Toolkit v4.0”	“31”
[ENI19b]	“ENISA’s Good Practices for Security of IoT Secure Software Development Lifecycle”	“30”
[ENI17b]	“ENISA’s Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*”	“25”
[GSM18]	“GSMA’s IoT Security Assessment Checklist Version 3.0”	“24”
[ENI20a]*	“ENISA’s Procurement Guidelines for Cybersecurity in Hospitals Good practices for the security of Healthcare services*”	“23”
[CSA15]	“CSA’s Security Guidance for Early Adopters of the Internet of Things (IoT)”	“22”
[IIC16]	“IIC’s Industrial Internet of Things Volume G4: Security Framework*”	“18”
[ETS20]	“ETSI European Standard (EN) 303.645 V2.1.1 Cyber Security for Consumer Internet of Things: Baseline Requirements”	“17”
[OTA18]	“OTA’s IoT Security & Privacy Trust Framework v2.5”	“16”
[ENI20b]	“ENISA’s Guidelines for Securing the Internet of Things Secure supply chain for IoT”	“14”
[CSA16]	“CSA’s Identity and Access Management for the Internet of Things - Summary Guidance”	“12”
[IoT16]*	“Japan’s IoTAC IoT Security Guidelines Ver. 1.0”	“12”
[NHT16]	“US NHTSA’s Cybersecurity Best Practices for Modern Vehicles*”	“9”
[NIS20a]*	“NIST’s Foundational Cybersecurity Activities for IoT Device Manufacturers”	“9”
[DHS16]	“US DHS’s Strategic Principles for Securing the Internet of Things (IoT) Version 1.0”	“8”
[DCM18a]	“UK DCMS’s Code of Practice for Consumer IoT Security”	“6”
[AIO16]	“AIOTI’s Report on Workshop on Security and Privacy in the Hyper-Connected World”	“5”
[Com20]	“Australian Government’s Code of Practice Securing the Internet of Things for Consumers”	“5”
[NEM18]	“NEMA’s Cyber Hygiene Best Practices”	“4”
[BIT16]	“BITAG’s Internet of Things (IoT) Security and Privacy Recommendations”	“2”
[IEE17]	“IEEE’s Internet of Things (IoT) Security Best Practices‟	“2”
[CSD19]	“CSDE’s The C2 Consensus on IoT Device Security Baseline Capabilities‟	“1”

Informative Reference	Name of Informative Reference	Total # of Unique in-Scope IoT Security Requirements Mapped

"Note, the informative references marked with an asterix resulted the most relevant to IoT security risk management strategy"

Furthermore, based on the information disseminated by the author through the research paper [Pop+21a], for each "IoTSRM2" domain, this subchapter provides "the associated IoTSRM2 objectives" [Pop+21a]. Additionally, for each "IoTSRM2" objective, it describes "the IoTSRM2 controls consistent with the intended information granularity from the methodology for developing the IoTSRM2 (see Chapter 5.1), which captures the following levels of detail: expected IoT security related activities/actions from IoT adopters, integration points of IoT security related expected 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" [Pop+21a]. Moreover, for each "IoTSRM2" control, it provides "the corresponding informative references with the unique identifiers of the in-scope IoT security requirements that are applicable" [Pop+21a]. Also, for each objective of each "IoTSRM2" domain, this subchapter provides "the unique identifier of the corresponding in-scope NIST CSF Subcategory, and the prioritization of IoTSRM2 controls based on their adjusted weights" [Pop+21a] (see Chapter 5.1). It is worth noting that "the adjusted weight for each IoTSRM2 control is calculated using Equations (5.10) and (5.11)" [Pop+21a] (see Chapter 5.1).

5.2.1. Domain: Asset Management (AM)

Based on the information disseminated by the author through the research paper [Pop+21a], "the Asset Management domain of IoTSRM2 comprises the following two objectives" [Pop+21a]:

- "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 [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.2 provides the description of this control together with "11 informative references and 23 unique identifiers of the in-scope IoT security requirements that apply to it" [Pop21].

Table 5.2. IoTSRM2 control for “Hardware inventory” objective. Adapted from [Pop+21a]

Control Description	Informative References
“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” [Pop+21a].	• **[Age20a]**: “12” • **[CSA15]**: “5.2.1.1, 5.5.2, 5.5.3.1” • **[CSA16]**: “14” • **[CSA19a]**: “ACT-01, ACT-03, ACT-04, ACT-05, GVN-01, OPA-01, TSP-02” • **[DHS16]**: “Promote Transparency across IoT: software bill of materials” • **[ENI18b]**: “PS-11, PS-12, PS-14” • **[ENI20a]**: “GP 28” • **[ENI20b]**: “PRO-13” • **[ETS20]**: “Provision 5.8-3” • **[NIS20a]**: “4.2.3, 4.2.6” • **[OTA18]**: “9, 11”

“Software inventory (AM.B)”

The “Software inventory” objective “has one IoTSRM2 control”, namely “IoT software assets inventory” control [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.3 provides the description of this control together with “10 informative references and 20 unique identifiers of the in-scope IoT security requirements that apply to it” [Pop21].

Table 5.3. IoTSRM2 control for “Software inventory” objective. Adapted from [Pop+21a]

Control Description	Informative References
“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	• **[Age20a]**: “12” • **[CSA15]**: “5.2.1.1, 5.5.3.1” • **[CSA19a]**: “ACT-01, ACT-03, ACT-05, GVN-01, TSP-02” • **[DHS16]**: “Promote Transparency across IoT: software bill of materials” • **[ENI18b]**: “PS-11, PS-12, PS-14” • **[ENI20a]**: “GP 28” • **[ENI20b]**:” PRO-05, PRO-13” • **[IoT16]**: “Principle 2: Key concept 3” • **[NIS20a]**: “4.2.3, 4.2.6”

Control Description	Informative References
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" [Pop+21a].	• **[OTA18]**: "9, 11"

Then, based on the information disseminated by the author through the research paper [Pop+21a], "for each IoTSRM2 objective of the Asset Management domain", Table 5.4 provides "the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 control with its adjusted weight" [Pop+21a]. 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" [Pop+21a].

Table 5.4. Prioritized IoTSRM2 controls for each objective of "Asset Management" domain [Pop+21a]

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%"

5.2.2. Domain: Business Environment (BE)

Based on the information disseminated by the author through the research paper [Pop+21a], "the Business Environment domain of IoTSRM2 consists of the following two objectives" [Pop+21a]:

- "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 [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.5 provides the description of this control together with "14 informative references and 33 unique identifiers of the in-scope IoT security requirements that apply to it" [Pop21].

Table 5.5. IoTSRM2 control for "Dependencies and critical functions" objective. Adapted from [Pop+21a]

Control Description	Informative References
"Criticality and impact analysis (BE.A.1)": "All IoT enabled services (e.g., internal services, customer services) along with the enablers for 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" [Pop+21a].	• **[Age20a]**: "12, 23, 44" • **[AIO16]**: "Basic Requirements on IoT HARDWARE AND COMPONENTS: Standardisation" • **[CSA19a]**: "GVN-02, SOP-01, SOP-02, TMM-04" • **[DHS16]**: "Connect Carefully and Deliberately: Advise IoT consumers on the intended purpose of any network connections, Promote Transparency across IoT: software bill of materials" • **[ENI17b]**: "6.2.4" • **[ENI18b]**: "PS-07, PS-08, PS-19, TM-10, TM-13" • **[ENI19b]**: "PR-02" • **[ENI20a]**: "GP 7, GP 12" • **[ENI20b]**: "ACT-03, PRO-04, PRO-05, PRO-13" • **[IIC16]**: "5.1" • **[IoT16]**: "Principle 2: Key concept 3, Principle 2: Key concept 5, Principle 5: Key concept 19" • **[NHT16]**: "8" • **[NIS20a]**: "4.2.1, 4.2.3, 4.2.6" • **[OTA18]**: "11, 21"

"Critical service resilience (BE.B)"

The "Critical service resilience" objective "has one IoTSRM2 control", namely "Resiliency requirements" control [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.6 provides the description of this control together with "15 informative references and 32 unique identifiers of the in-scope IoT security requirements that apply to it" [Pop21].

Table 5.6. IoTSRM2 control for "Critical service resilience" objective. Adapted from [Pop+21a]

Control Description	Informative References
"Resiliency requirements (BE.B.1)": "Cybersecurity, reliability, continuity, and recovery requirements for critical IoT enabled services across the entire disruption lifecycle, are established,	• **[Age20a]**: "12, 23, 44" • **[CSA15]**: "5.5.5" • **[CSA16]**: "15" • **[CSA19a]**: "BCN-01"

Control Description	Informative References
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" [Pop+21a].	• **[DHS16]**: "Promote Transparency across IoT: software bill of materials" • **[ENI17b]**: "6.2.4, 6.2.5" • **[ENI18b]**: "OP-01, TM-09, TM-12, TM-15, TM-16, TM-17" • **[ENI19b]**: "PE-08, PR-33, TC-27" • **[ENI20a]**: "GP 6, GP 17, GP 22, GP 23" • **[ENI20b]**: "ACT-03, PRO-13" • **[IIC16]**: "6.2, 6.3, 6.5" • **[IoT20a]**: "2.4.3.18, 2.4.3.23" • **[NEM18]**: "7" • **[NHT16]**: "6.5" • **[OTA18]**: "21"

Then, based on the information disseminated by the author through the research paper [Pop+21a], "for each IoTSRM2 objective of the Business Environment domain", Table 5.7 provides "the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 control with its adjusted weight" [Pop+21a]. 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" [Pop+21a].

Table 5.7. Prioritized IoTSRM2 controls for each objective of "Business Environment" domain [Pop+21a]

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%"

5.2.3. Domain: Governance (GV)

Based on the information disseminated by the author through the research paper [Pop+21a], "the Governance domain of IoTSRM2 consists of the following four objectives" [Pop+21a]:

- “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” [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.8 provides the description of these controls together with “the informative references and the unique identifiers of the in-scope IoT security requirements that apply to each of them” [Pop21]. The “IoT security policy”, “Privacy policy”, “Vulnerability disclosure policy”, and “End-of-Life policy” controls:

- “have 16, 13, 11, and 10 informative references, respectively” [Pop21];
- “have 39, 26, 16, and 16 unique identifiers of in-scope IoT security requirements, respectively” [Pop21].

Table 5.8. IoTSRM2 controls for “Security related policies” objective. Adapted from [Pop+21a]

Control Description	Informative References
“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” [Pop+21a].	• **[Age20a]**: “4, 5, 7” • **[AIO16]**: “Basic Requirements on INTERFACES, COMMUNICATION, CLOUD:Standardization” • **[BIT16]**: “7.10” • **[Com20]**: “7” • **[CSA15]**: “5.4.1, 5.5, 5.5.5.1” • **[CSA19a]**: “TSP-04” • **[DCM18a]**: “5” • **[ENI17b]**: “GP-PS-10, 6.2.1” • **[ENI18b]**: “PS-18” • **[ENI19b]**: “PR-12” • **[ENI20a]**: “GP 3, GP 5” • **[ETS20]**: “Provision 5.3-8, Provision 5.3-11, Provision 5.5-8” • **[GSM18]**: “CLP12_7.4.1.1, CLP12_5.11.1.1, CLP12_5.12.1.1” • **[IIC16]**: “7.1, 7.8” • **[IoT16]**: “Principle 1: Key concept 1, Principle 1: Key concept 2” • **[IoT20a]**: “2.4.3.4, 2.4.3.5, 2.4.3.6, 2.4.8.10”

Control Description	Informative References
“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” [Pop+21a].	• **[Age20a]**: “20, 22, 24, 25, 32, 35, 36” • **[BIT16]**: “7.7” • **[Com20]**: “5” • **[CSA15]**: “5.1.4, 5.1.5” • **[DCM18a]**: “8” • **[ENI17b]**: “GP-TM-13” • **[ENI18b]**: “PS-06” • **[ENI20a]**: “GP 10“ • **[ETS20]**: “Provision 5.8-3, Provision 6-1, Provision 6-5” • **[GSM18]**: “CLP11_11.6.5.3, CLP11_11.6.5.7” • **[IoT20a]**: “2.4.12.5” • **[NIS20a]**: “4.2.3” • **[OTA18]**: “18, 20, 22, 24”
“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 vulnerability disclosure program” [Pop+21a].	• **[Com20]**: “2” • **[CSA19a]**: “SDV-05” • **[DCM18a]**: “2” • **[DHS16]**: “Promote Security Updates and Vulnerability Management: coordinated disclosure of vulnerabilities” • **[ENI17b]**: “GP-OP-06” • **[ETS20]**: “Provision 5.2-1, Provision 5.2-2 • **[IEE17]**: 10” • **[IoT20a]**: “2.4.3.11, 2.4.3.12, 2.4.3.13, 2.4.3.14, 2.4.3.16, 2.4.3.17” • **[NHT16]**: “6.4” • **[NIS20a]**: “4.2.6”
“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” [Pop+21a].	• **[Age20a]**: “1, 21” • **[Com20]**: “3” • **[CSA19a]**: “EOL-01” • **[CSD19]**: “5.2.2” • **[DCM18a]**: “3” • **[ENI17b]**: “GP-OP-02, 6.2.6” • **[ETS20]**: “Provision 5.3-13, Provision 5.3-14” • **[IEE17]**: “4” • **[IoT20a]**: “2.4.5.22, 2.4.5.35” • **[NIS20a]**: “4.2.2, 4.2.5” • **[OTA18]**: “19”

"Structures and responsibilities (GV.B)"

The "Structures and responsibilities" objective "has two IoTSRM2 controls" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.9 provides the description of these controls together with "the informative references and the unique identifiers of the in-scope IoT security requirements that apply to each of them" [Pop21]. The "IoT security governance structures and responsibilities" and "IoT security operations roles and responsibilities" controls:

- "have 3 and 13 informative references, respectively" [Pop21];
- "have 8 and 23 unique identifiers of in-scope IoT security requirements, respectively" [Pop21].

Table 5.9. IoTSRM2 controls for "Structures and responsibilities" objective. Adapted from [Pop+21a]

Control Description	Informative References
"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 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" [Pop+21a].	• **[CSA19a]**: "GVN-01, UPD-01" • **[IoT20a]**: "2.4.3.1, 2.4.3.2" • **[GSM18]**: "CLP11_11.7.2.2, CLP11_11.7.2.3, CLP11_11.7.2.4, CLP11_11.7.2.5"
"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" [Pop+21a].	• **[Com20]**: "2" • **[CSA15]**: "5.1.6, 5.5.4" • **[CSA19a]**: "BCN-01, IMT-02" • **[DCM18a]**: "2" • **[ENI17b]**: "GP-OP-11" • **[ENI18b]**: "OP-08, OP-11" • **[ENI19b]**: "PE-05, PE-09, PE-12" • **[ENI20a]**: "GP 1" • **[GSM18]**: "CLP11_11.6.3.5, CLP11_11.7.2.1" • **[IoT16]**: "Principle 5: Key concept 20" • **[IoT20a]**: "2.4.3.19, 2.4.3.20, 2.4.3.21, 2.4.12.12" • **[NHT16]**: "6.2"

Control Description	Informative References
	• **[NIS20a]**: "4.2.1, 4.2.4"

"Regulatory requirements (GV.C)"

The "Regulatory requirements" objective "has one IoTSRM2 control", namely "Cybersecurity regulatory framework" control [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.10 provides the description of this control together with "8 informative references and 12 unique identifiers of the in-scope IoT security requirements that apply to it" [Pop21].

Table 5.10. IoTSRM2 control for "Regulatory requirements" objective. Adapted from [Pop+21a]

Control Description	Informative References
"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" [Pop+21a].	• **[Age20a]**: "31" • **[CSA15]**: "5.1.1.1" • **[CSA19a]**: "CLS-04, GVN-02, RSM-01" • **[ENI17b]**: "6.2.1" • **[ENI18b]**: "PS-06, TM-07" • **[GSM18]**: "CLP11_11.6.4.2" • **[IIC16]**: "5.1, 10.4" • **[OTA18]**: "30"

"Governance and risk management plans (GV.D)"

The "Governance and risk management plans" objective "has seven IoTSRM2 controls" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.11 provides the description of these controls together with "the informative references and the unique identifiers of the in-scope IoT security requirements that apply to each of them" [Pop21]. The "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", and "IoT End-of-Life plan" controls:

- "have 16, 10, 11, 4, 3, 14, and 16 informative references, respectively" [Pop21];
- "have 70, 15, 16, 4, 6, 29, and 19 unique identifiers of in-scope IoT security requirements, respectively" [Pop21].

Table 5.11. IoTSRM2 controls for "Governance and risk management plans" objective. Adapted from [Pop+21a]

Control Description	Informative References
"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" [Pop+21a].	• **[Age20a]**: "5, 25, 30" • **[Com20]**: "11" • **[CSA15]**: "5.1.1, 5.2.1.2, 5.5, 5.5.1, 5.5.3.2, 5.7" • **[CSA16]**: "01, 03, 06, 08, 09, 11, 16" • **[CSA19a]**: "BCN-01, RSM-01, SDV-15, UPD-03" • **[DCM18a]**: "11, 12" • **[ENI17b]**: "GP-TM-10, GP-TM-11, 6.2.1, 6.2.3" • **[ENI18b]**: "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" • **[ENI19b]**: "PE-11, PR-16, PR-18, PR-20, PR-21" • **[ENI20a]**: "GP 6" • **[ENI20b]**: "PRO-04, PRO-12 • **[ETS20]**: Provision 5.11-3, Provision 5.11-4" • **[GSM18]**: "CLP11_11.6.1.4, CLP11_11.7.1.3, CLP12_6.7.1.1" • **[IIC16]**: "7.2, 7.7, 7.8" • **[IoT20a]**: "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"
"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" [Pop+21a].	• **[ENI17b]**: "6.2.5" • **[ENI19b]**: "PE-04, PE-08, PE-10, PE-13" • **[NHT16]**: "6.2"
"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	• **[ENI19b]:** "PR-14" • **[ENI20b]:** "PRO-04" • **[IIC16]:** "5,5" • **[NIS20a]:** "4.1"

Control Description	Informative References
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" [Pop+21a].	
"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" [Pop+21a].	• **[Age20a]:** "41, 43" • **[CSA16]:** "21, 23" • **[CSA19a]:** "TRN-01, TRN-02" • **[ENI17b]:** "GP-OP-10, 6.2.2" • **[ENI18b]:** "OP-19, OP-20, OP-21, OP-23" • **[ENI19b]:** "PE-01, PR-30" • **[ENI20a]:** "GP 21, GP 27" • **[ENI20b]:** "ACT-06, ACT-07, PRO-10" • **[ETS20]:** "Provision 5.12-2, Provision 5.12-3" • **[IoT16]:** "Principle 2: Key concept 7" • **[IoT20a]:** 2.4.12.11, 2.4.12.12" • **[NHT16]:** "7" • **[NIS20a]:** "4.2, 4.2.3, 4.2.6" • **[OTA18]:** "39"
"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" [Pop+21a].	• **[Age20a]**: "40" • **[CSA15]**: "5.5.5" • **[CSA16]**: "15" • **[CSA19a]**: "IMT-02" • **[ENI17b]**: "GP-OP-05" • **[ENI18b]**: "OP-10, OP-11, OP-12" • **[ENI20a]**: "GP 22, GP 23" • **[GSM18]**: "CLP11_11.5.3.2, CLP11_11.5.3.4" • **[IIC16]**: "10.1.1" • **[IoT20a]**: "2.4.3.8, 2.4.3.21" • **[NHT16]**: "6.5"
"IoT vulnerability management plan (GV.D.6)": "An IoT vulnerability management plan, which is aligned with and supports the	• **[Age20a]**: "2, 9" • **[CSA19a]**: "OPA-01, VLN-01" • **[DHS16]**: "Promote Security Updates and Vulnerability Management: coordinating

Control Description	Informative References
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” [Pop+21a].	software updates among third-party vendors, Promote Transparency across IoT: publicly disclosed mechanism for using vulnerability reports” • **[ENI17b]**: “GP-OP-08” • **[ENI18b]**: “OP-14, OP-15, OP-16, OP-18” • **[ENI19b]**: “PR-08” • **[ENI20a]**: “GP 24, GP 26” • **[ENI20b]**: “TEC-01” • **[GSM18]**: “CLP11_11.5.3.3, CLP11_11.5.3.4, CLP12_6.6.1.4” • **[IEE17]**: “10” • **[IoT16]**: “Principle 5: Key Concept 17” • **[IoT20a]**: “2.4.3.7, 2.4.3.9, 2.4.13.5” • **[NEM18]**: “6,7” • **[NHT16]**: “6.4” • **[NIS20a]**: “4.2.4” • **[OTA18]**: “5, 8”
“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” [Pop+21a].	• **[Age20a]**: “33, 34” • **[CSA19a]**: “EOL-01” • **[DHS16]**: “Promote Security Updates and Vulnerability Management: end-of-life strategy” • **[ENI17b]**: “GP-OP-01, 6.2.6” • **[ENI18b]**: “OP-01” • **[ENI19b]**: “PR-17” • **[ENI20b]**: “PRO-10” • **[GSM18]**: “CLP12_5.10.1.1, CLP13_8.10.1.1” • **[IEE17]**: “4” • **[NIS20a]**: “3.4, 4.2.2, 4.2.5”

Then, based on the information disseminated by the author through the research paper [Pop+21a], “for each IoTSRM2 objective of the Governance domain”, Table 5.12 provides “the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 controls with their adjusted weights” [Pop+21a]. These “IoTSRM2” controls “are prioritized within each IoTSRM2 objective” [Pop+21a]. 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 [Pop+21a].

Table 5.12. Prioritized IoTSRM2 controls for each objective of "Governance" domain [Pop+21a]

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%"

5.2.4. Domain: Risk Assessment (RA)

Based on the information disseminated by the author through the research paper [Pop+21a], "the Risk Assessment domain of IoTSRM2 consists of the following four objectives" [Pop+21a]:

- "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" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.13 provides the description of these controls together with "the informative references and the unique identifiers of the in-scope IoT security requirements that apply to each of them" [Pop21]. The "Disclosure-based IoT vulnerability discovery" and "Assessment-based IoT vulnerability discovery" controls:

- "have 14 and 17 informative references, respectively" [Pop21];
- "have 20 and 61 unique identifiers of in-scope IoT security requirements, respectively" [Pop21].

Table 5.13. IoTSRM2 controls for "Vulnerability discovery" objective. Adapted from [Pop+21a]

Control Description	Informative References
"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" [Pop+21a].	• **[Age20a]**: "9" • **[AIO16]**: "Basic Requirements on IoT HARDWARE AND COMPONENTS: Information exchange" • **[Com20]**: "2" • **[CSA19a]**: "SDV-05" • **[DCM18a]**: "2" • **[DHS16]**: "Promote Transparency across IoT: publicly disclosed mechanism for using vulnerability reports, Build on Recognized Security Practices: information sharing platforms" • **[ENI17b]**: "GP-OP-06, GP-OP-07, GP-OP-08" • **[ETS20]**: "Provision 5.2-2, Provision 5.3-11" • **[GSM18]**: "CLP11_11.5.3.4" • **[IEE17]**: "10" • **[IoT16]**: "Principle 5: Key concept 18" • **[IoT20a]**: "2.4.3.7, 2.4.3.9" • **[NHT16]**: "6.3" • **[OTA18]**: "5, 39"
"Assessment-based IoT vulnerability discovery (RA.A.2)": "The attack surface of the organization's IoT footprint across its entire system	• **[Age20a]**: "8, 10, 12, 44" • **[CSA15]**: "5.1.7, 5.2.1.3, 5.5.4"

Control Description	**Informative References**
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, to achieve ongoing vulnerability monitoring and cybersecurity improvement" [Pop+21a].	• **[CSA19a]**: "GVN-03, PRV-02, PRV-04, RSM-02, SOP-02, TMM-01, TMM-02, TMM-04, VLN-01" • **[DHS16]**: "Promote Transparency across IoT: third party vendor risks, Promote Transparency across IoT: software bill of materials" • **[ENI17b]**: "GP-PS-09, GP-PS-11, GP-TM-57" • **[ENI18b]**: "PS-09, PS-19, PS-21, OP-04, OP-17, TM-10, TM-14, TM-15" • **[ENI19b]**: "PE-03, PR-26, PR-32, TC-21" • **[ENI20a]**: "GP 2, GP 8, GP 11, GP 19, GP 30" • **[ENI20b]**: "PRO-05, PRO-13" • **[ETS20]**: "Provision 5.2-3" • **[GSM18]**: "CLP11_11.7.4.3" • **[IIC16]**: "5.2, 5.4, 6.5, 7.8, 8.1, 11.1" • **[IoT16]**: "Principle 2: Key concept 4, Principle 2: Key concept 5, Principle 2: Key concept 6, Principle 5: Key concept 21" • **[IoT20a]**: "2.4.10.9, 2.4.13.5" • **[NEM18]**: "3, 6" • **[NHT16]**: "6.6.1, 6.6.3" • **[OTA18]**: "4, 10, 11"

"Threat identification (RA.B)"

The "Threat identification" objective "has two IoTSRM2 controls" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.14 provides the description of these controls together with "the informative references and the unique identifiers of the in-scope IoT security requirements that apply to each of them" [Pop21]. The "Intelligence-driven IoT threat identification" and "Assessment-based IoT threat identification" controls:

- "have 9 and 15 informative references, respectively" [Pop21];
- "have 10 and 40 unique identifiers of in-scope IoT security requirements, respectively" [Pop21].

Table 5.14. IoTSRM2 controls for "Threat identification" objective. Adapted from [Pop+21a]

Control Description	Informative References
"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" [Pop+21a].	• **[Age20a]**: "9" • **[CSA19a]**: "TMM-03" • **[DHS16]**: "Build on Recognized Security Practices: information sharing platforms" • **[ENI17b]**: "GP-OP-07" • **[ENI18b]**: "PS-22, OP-23" • **[ETS20]**: "Provision 5.3-11" • **[IoT16]**: "Principle 5: Key concept 18" • **[NHT16]**: "6.3" • **[OTA18]**: "5"
"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" [Pop+21a].	• **[Age20a]**: "8, 44" • **[CSA15]**: "5.1.7, 5.2.1.4, 5.5.4" • **[CSA19a]**: "PRV-02, PRV-04, RSM-02, TMM-01, SOP-02, VLN-01" • **[DHS16]**: "Promote Transparency across IoT: third party vendor risks" • **[ENI17b]**: "GP-PS-09, GP-PS-11" • **[ENI18b]**: "PS-09, PS-19, PS-21, PS-23, OP-17, TM-10, TM-14, TM-15" • **[ENI19b]**: "PR-26" • **[ENI20a]**: "GP 11, GP 13, GP 19" • **[GSM18]**: "CLP11_11.7.4.3" • **[IIC16]**: "5.2, 6.5, 7.8, 8.1, 11.1" • **[IoT16]**: "Principle 2: Key concept 4, Principle 2: Key concept 5, Principle 2: Key concept 6" • **[IoT20a]**: "2.4.10.9" • **[NEM18]**: "3, 6" • **[NHT16]**: "6.6.1" • **[OTA18]**: "10"

"Risk analysis (RA.C)"

The "Risk analysis" objective "has one IoTSRM2 control", namely "IoT risk identification and analysis" control [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.15 provides the description of this control together with "14 informative references and 37 unique identifiers of the in-scope IoT security requirements that apply to it" [Pop21].

Table 5.15. IoTSRM2 control for "Risk analysis" objective. Adapted from [Pop+21a]

Control Description	Informative References
"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" [Pop+21a].	• **[Age20a]**: "8, 9, 44" • **[AIO16]**: "Basic Requirements on PRACTICAL PRIVACY IN IoT: Accountability & Risk Impact Assessment by Design" • **[CSA15]**: "5.1.7, 5.2.1.5" • **[CSA19a]**: "PRV-02, PRV-04, RSM-02, SOP-01, SOP-02, TMM-01, VLN-01" • **[DHS16]**: "Promote Transparency across IoT: third party vendor risks" • **[ENI17b]**: "GP-PS-09, GP-PS-11" • **[ENI18b]**: "PS-09, PS-19, PS-21, PS-23, TM-10, TM-14, TM-15" • **[ENI19b]**: "PR-26" • **[ENI20a]**: "GP 11, GP 19" • **[IIC16]**: "5.3, 6.5" • **[IoT16]**: "Principle 2: Key concept 4, Principle 2: Key concept 5, Principle 2: Key concept 6, Principle 5: Key concept 18" • **[IoT20a]**: "2.4.10.9" • **[NHT16]**: "6.6.1" • **[OTA18]**: "4, 5, 10, 21"

"Risk responses (RA.D)"

The "Risk responses" objective "has one IoTSRM2 control", namely "Cybersecurity risk register and IoT risk responses" control [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.16 provides the description of this control together with "12 informative references and 23 unique identifiers of the in-scope IoT security requirements that apply to it" [Pop21].

Table 5.16. IoTSRM2 control for "Risk responses" objective. Adapted from [Pop+21a]

Control Description	Informative References
"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,	• **[Age20a]**: "9" • **[CSA15]**: "5.1.7" • **[CSA19a]**: "PRV-02, PRV-04, RSM-02, SOP-01, TMM-01, VLN-01"

Control Description	Informative References
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 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" [Pop+21a].	• **[DHS16]**: "Promote Transparency across IoT: third party vendor risks" • **[ENI17b]**: "GP-PS-09, TC-27" • **[ENI18b]**: "PS-09, PS-19, PS-21, TM-14" • **[ENI20a]**: "GP 11, GP 19" • **[IIC16]**: "5.6, 6.5" • **[IoT20a]**: "2.4.10.9" • **[NHT16]**: "6.6.1" • **[OTA18]**: "4, 10"

Then, based on the information disseminated by the author through the research paper [Pop+21a], "for each IoTSRM2 objective of the Risk Assessment domain", Table 5.17 provides "the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 controls with their adjusted weights" [Pop+21a]. These "IoTSRM2" controls "are prioritized within each IoTSRM2 objective" [Pop+21a]. 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 [Pop+21a].

Table 5.17. Prioritized IoTSRM2 controls for each objective of "Risk Assessment" domain [Pop+21a]

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%"

5.2.5. Domain: Risk Management Strategy (RM)

Based on the information disseminated by the author through the research paper [Pop+21a], "the Risk Management Strategy domain of IoTSRM2 consists of the following two objectives" [Pop+21a]:

- "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 [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.18 provides the description of this control together with "6 informative references and 6 unique identifiers of the in-scope IoT security requirements that apply to it" [Pop21].

Table 5.18. IoTSRM2 control for "Risk appetite and tolerances" objective. Adapted from [Pop+21a]

Control Description	Informative References
"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" [Pop+21a].	• **[CSA19a]**: "RSM-01" • **[ENI18b]**: "PS-18" • **[IIC16]**: "5.1" • **[IoT20a]**: "2.4.3.4" • **[NEM18]**: "Risk Tolerance" • **[OTA18]**: "4"

"Context-informed risk tolerances (RM.B)"

The "Context-informed risk tolerances" objective "has one IoTSRM2 control", namely "Context-informed IoT security risk tolerances" control [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.19 provides the description of this control together with "6 informative references and 6 unique identifiers of the in-scope IoT security requirements that apply to it" [Pop21].

Table 5.19. IoTSRM2 control for "Context-informed risk tolerances" objective. Adapted from [Pop+21a]

Control Description	Informative References
"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" [Pop+21a].	• **[CSA19a]**: "RSM-01" • **[ENI18b]**: "PS-18" • **[IIC16]**: "5.1" • **[IoT20a]**: "2.4.3.4" • **[NEM18]**: "Risk Tolerance" • **[NIS20a]**: "4.2.1"

Then, based on the information disseminated by the author through the research paper [Pop+21a], "for each IoTSRM2 objective of the Risk Management Strategy domain", Table 5.20 provides "the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 control with its adjusted weight" [Pop+21a]. 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" [Pop+21a].

Table 5.20. Prioritized IoTSRM2 controls for each objective of "Risk Management Strategy" domain [Pop+21a]

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%"

5.2.6. Domain: Supply Chain Risk Management (SC)

Based on the information disseminated by the author through the research paper [Pop+21a], "the Supply Chain Risk Management domain of IoTSRM2 consists of the following two objectives" [Pop+21a]:

- "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" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.21 provides the description of these controls together with "the informative references and the unique identifiers of the in-scope IoT security requirements that apply to each of them" [Pop21]. The "IoT supply chain risk management plan" and "IoT supply chain risk assessment" controls:

- "have 11 and 12 informative references, respectively" [Pop21];
- "have 25 and 16 unique identifiers of in-scope IoT security requirements, respectively" [Pop21].

Table 5.21. IoTSRM2 controls for "Supplier assessment" objective. Adapted from [Pop+21a]

Control Description	Informative References
"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	• **[Age20a]**: "12" • **[CSA19a]**: "SDV-15" • **[ENI17b]**: "GP-OP-14" • **[ENI18b]**: "OP-26, TM-07" • **[ENI19b]**: "PR-01, PR-02, PR-03" • **[ENI20b]**: "ACT-01, ACT-03, ACT-04, GP 11, GP 16, GP 17, GP 18, PRO-03, PRO-04, PRO-05"

Control Description	Informative References
have and maintain cyber supply chain risk management plans to effectively address cyber supply chain risks across their whole IoT supply chains" [Pop+21a].	• **[GSM18]**: "CLP12_5.11.1.2, CLP12_6.7.1.1, CLP13_9.7.1.2" • **[IIC16]**: "5.1, 6.1" • **[IoT20a]**: "2.4.3.6" • **[NHT16]**: "6.6.1"
"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" [Pop+21a].	• **[Age20a]**: "11" • **[BIT16]**: "7.10" • **[CSA15]**: "5.1.7" • **[CSA16]**: "04" • **[CSA19a]**: "RSM-02" • **[DHS16]**: "Promote Transparency across IoT: third party vendor risks" • **[ENI18b]**: "PS-19, TM-10" • **[ENI19b]**: "PR-04" • **[IIC16]**: "5.2, 6.5, 7.8, 8.1" • **[NHT16]**: "6.6" • **[NIS20a]**: "4.2.3" • **[OTA18]**: "10"

"Supplier contract management (SC.B)"

The "Supplier contract management" objective "has two IoTSRM2 controls" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], Table 5.22 provides the description of these controls together with "the informative references and the unique identifiers of the in-scope IoT security requirements that apply to each of them" [Pop21]. The "IoT supplier contract management plan" and "IoT trustworthiness requirements" controls:

- "have 13 and 11 informative references, respectively" [Pop21];
- "have 24 and 44 unique identifiers of in-scope IoT security requirements, respectively" [Pop21].

Table 5.22. IoTSRM2 controls for "Supplier contract management" objective. Adapted from [Pop+21a]

Control Description	Informative References
"IoT supplier contract management plan (SC.B.1)": "An organization-wide IoT supplier contract management plan, which is aligned with and part of 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 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" [Pop+21a].	• **[Age20a]**: "1, 21, 29" • **[AIO16]**: "Basic Requirements on APPLICATIONS: Accountability & Liability, Basic Requirements on PRACTICAL PRIVACY IN IoT: Accountability & Risk Impact Assessment by Design" • **[CSA15]**: "5.2.2.1" • **[CSA19a]**: "OPA-05, RMT-01" • **[ENI17b]**: "GP-OP-02, 6.2.6, 6.2.7" • **[ENI18b]**: "OP-05, OP-27, TM-30" • **[ENI19b]**: "PR-06, PR-07" • **[ENI20a]**: "GP 23" • **[ENI20b]**: "PRO-08" • **[IIC16]**: "5.1" • **[IoT16]**: "Principle 5: Key concept 20" • **[IoT20a]**: "2.4.5.36" • **[NIS20a]**: "4.2.1, 4.2.3, 4.2.4"
"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 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" [Pop+21a].	• **[Age20a]**: "3, 4, 12, 22, 24, 26, 28, 31, 36, 44" • **[CSA19a]**: "CLS-04, GVN-02, RMT-02" • **[DHS16]**: "Promote Transparency across IoT: software bill of materials" • **[ENI17b]**: "GP-OP-12, GP-OP-13, GP-TM-13, 6.2.1, 6.2.3, 6.2.4, 6.2.5" • **[ENI18b]**: "PS-06, OP-01, OP-02, OP-03, OP-26, TM-08, TM-09" • **[ENI20a]**: "GP 30" • **[ENI20b]**: "ACT-01, ACT-03, ACT-08, PRO-05, PRO-13" • **[ETS20]**: "Provision 6-2, Provision 6-3" • **[IIC16]**: "6.2, 6.3, 6.5" • **[IoT16]**: "Principle 2: Key concept 3" • **[OTA18]**: "1, 22, 25, 30"

Then, based on the information disseminated by the author through the research paper [Pop+21a], "for each IoTSRM2 objective of the Supply Chain Risk

Management domain", Table 5.23 provides "the unique identifier of the in-scope NIST CSF Subcategory and the associated IoTSRM2 controls with their adjusted weights" [Pop+21a]. These "IoTSRM2" controls "are prioritized within each IoTSRM2 objective" [Pop+21a]. 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 [Pop+21a].

Table 5.23. Prioritized IoTSRM2 controls for each objective of "Supply Chain Risk Management" domain [Pop+21a]

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%"

5.3. Evaluation of Selected Informative References of IoTSRM2

Based on the information disseminated by the author through the research paper [Pop+21a] and the PhD report [Pop21], this subchapter provides "a critical evaluation of selected informative references of IoTSRM2 based on their percentage-wise linkage to IoTSRM2" [Pop+21a]. 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" [Pop+21a] (see Chapter 5.1). Thus, based on the information disseminated by the author through the research paper [Pop+21a], the informative references that are selected in-scope [Pop+21a] for the critical evaluation are: [Age20a], [CSA19a], [ENI18b], [ENI20a], [IoT16], [IoT20a], and [NIS20a].

Furthermore, this subchapter is structured in seven sub-subchapters and includes the overall evaluation of selected informative references (see Chapter 5.3.1) and individual evaluations of selected informative references for each IoTSRM2 domain (see Chapters 5.3.2-5.3.7). With respect to the overall evaluation of selected informative references, it outlines two critical evaluations. First, the selected informative references are critically evaluated relative to "their percentage-wise linkage to the IoTSRM2 domains and to the entire IoTSRM2" [Pop+21a]. Second, the selected informative references are critically evaluated based on their number of in-scope IoT security requirements for each IoTSRM2 domain [Pop+21a]. Then, with respect to the individual evaluations of selected informative references for each

IoTSRM2 domain, the selected informative references are critically evaluated "relative to their percentage-wise linkage to the objectives of the IoTSRM2 domain and to the entire IoTSRM2 domain" [Pop21].

5.3.1. Overall Evaluation

The selected informative references are critically evaluated relative to "their percentage-wise linkage to the IoTSRM2 domains and to the entire IoTSRM2" [Pop+21a]. Based on the information disseminated by the author through the research paper [Pop+21a], Fig. 5.3 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" [Pop+21a];
- "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" [Pop+21a].

Based on the information disseminated by the author through the research paper [Pop+21a], "with respect to the percentage-wise linkage of the selected informative references to each IoTSRM2 domain", while Refs. [Age20a], [CSA19a], [ENI18b], and [IoT20a] "each resulted as the most linked to some of the IoTSRM2 domains", Refs. [Age20a], [ENI20a], [IoT16], [IoT20a], and [NIS20a] "each resulted as the least linked to some of the IoTSRM2 domains" [Pop+21a]. First, about Ref. [Age20a], 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 [Pop+21a]. Second, with respect to Ref. [CSA19a], "from the selected references, it resulted in being the most linked to" the "Asset Management", "Risk Assessment", and "Risk Management Strategy" domains [Pop+21a]. Third, regarding Ref. [ENI18b], "from the selected references, it resulted in being the most linked to" the "Business Environment", "Governance", and "Risk Management Strategy" domains [Pop+21a]. Fourth, about Ref. [ENI20a], "from the selected references, it resulted in being the least linked to" the "Risk Management Strategy" domain [Pop+21a]. Then, about Ref. [IoT16], "from the selected references, it resulted in being the least linked to" the "Governance", "Risk Management Strategy", and "Supply Chain Risk Management" domains [Pop+21a]. Next, with regards to Ref. [IoT20a], 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 [Pop+21a]. In addition, with regards to Ref. [NIS20a], "from the selected references, it resulted in being the least linked to" the "Risk Assessment" domain [Pop+21a]. Furthermore, the evaluation of selected informative references relative to their percentage-wise linkage to IoTSRM2 domains is later discussed separately for each IoTSRM2 domain [Pop21].

Based on the information disseminated by the author through the research paper [Pop+21a], "with respect to the percentage-wise linkage of the selected informative references to the entire IoTSRM2", Refs. [ENI18b], [CSA19a], and [Age20a] "resulted in being the top three most linked to IoTSRM2, in that order", whereas Refs. [IoT16], [NIS20a], and [ENI20a] "resulted in being the top three least linked to IoTSRM2, in that order" [Pop+21a]. 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" [Pop+21a].

Hence, with respect to Ref. [ENI18b], "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" [Pop+21a]. About Ref. [CSA19a], "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" [Pop+21a]. Regarding Ref. [Age20a], "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" [Pop+21a].

Then, with respect to Ref. [IoT16], "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 Ref. [IoT20a], it is the least linked to" the "Supply Chain Risk Management" domain [Pop+21a]. With regards to Ref. [NIS20a], "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" [Pop+21a]. As for Ref. [ENI20a], "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 Ref. [Age20a], it is the third least linked to" the "Risk Assessment" domain of "IoTSRM2" [Pop+21a].

Thus, based on the information disseminated by the author through the research paper [Pop+21a], "the resulting outcomes reflect the inclusion criteria of the selected informative references" [Pop+21a] (see Chapter 5.1). In addition, it is worth noting that "Ref. [ENI18b] has the strongest links to IoTSRM2 among all 25 informative references, and Ref. [IoT16] is the least linked to IoTSRM2 among the selected informative references" [Pop+21a].

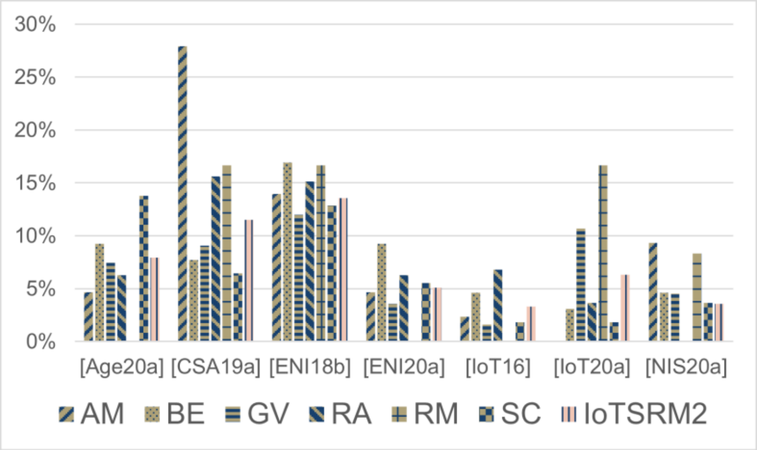


Fig. 5.3. Percentage-wise evaluation of selected informative references of IoTSRM2 [Pop+21a]

Furthermore, based on the information disseminated by the author through the research paper [Pop+21a], Fig. 5.4 outlines "the focus of each of the selected informative references from a strategic perspective, relative to each of the IoTSRM2 domains" [Pop+21a]. This is based on "the number of in-scope IoT security requirements corresponding to each selected informative reference for the IoTSRM2 domain in question" [Pop+21a]. First, Ref. [Age20a], the same as Ref. [ENI18b], "is the most focused on" the "Governance" domain, and "it is the least focused on" the "Risk Management Strategy" domain [Pop+21a]. Next, Ref. [CSA19a], the same as Refs. [ENI20a] and [IoT16], "is the most focused on" the "Risk Assessment" domain, and "it is the least focused on" the "Risk Management Strategy" domain [Pop+21a]. Then, Ref. [IoT20a] "is the most focused on" the "Governance" domain, and "it is the least focused on" the "Asset Management" domain [Pop+21a]. In addition, Ref. [NIS20a] "is the most focused on" the "Governance" domain, and "it is the least focused on" the "Risk Assessment" domain [Pop+21a]. 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 [Pop+21a].

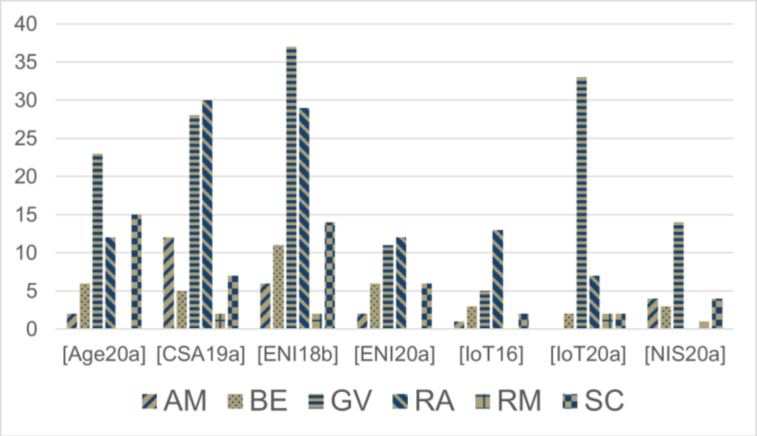


Fig. 5.4. Evaluation of selected informative references of IoTSRM2 [Pop+21a]

5.3.2. Evaluation for Asset Management (AM)

Based on the information disseminated by the author through the PhD report [Pop21], Fig. 5.3 and 5.5 provide the percentage score for the linkage of each selected informative reference to the "Asset Management" domain of "IoTSRM2" [Pop21]. Thus, from the selected informative references, Refs. [CSA19a], [ENI18b], and [NIS20a] "resulted in being the top three most linked to" the "Asset Management" domain, in that order, whereas Refs. [IoT20a], [IoT16], [ENI20a], and [Age20a] "resulted in being the top four least linked to" the "Asset Management" domain, in that order, where both Refs. [Age20a] and [ENI20a] share the same position [Pop21]. The rationale behind these outputs is "based on the percentage scores of the objectives corresponding to" the "Asset Management" domain of IoTSRM2, where the "Hardware inventory (AM.A)" objective "has a slightly higher number of in-scope IoT security requirements mapped to it than" the "Software inventory (AM.B)" objective [Pop21].

Hence, with respect to Ref. [CSA19a], "its very high percentage score is because, from the selected informative references, it is the most linked to" both the "Hardware inventory (AM.A)" and "Software inventory (AM.B)" objectives of the "Asset Management" domain [Pop21]. About Ref. [ENI18b], "its high percentage score is because, from the selected informative references, it is the second most linked to" both the "Hardware inventory (AM.A)" and "Software inventory (AM.B)" objectives of the "Asset Management" domain [Pop21]. Regarding Ref. [NIS20a], "its fairly high percentage score is because, from the selected informative references, it is the third most linked to" both the "Hardware inventory (AM.A)" and "Software inventory (AM.B)" objectives of the "Asset Management" domain [Pop21].

Next, with respect to Ref. [IoT20a], "its very low percentage score is because it is very much not focused on the strategic side of" the "Asset Management" domain and, "from the selected informative references", it has no apparent link to the "Hardware inventory (AM.A)" objective nor to the "Software inventory (AM.B)" objective of the "Asset Management" domain [Pop21]. About Ref. [IoT16], "its low percentage score is because", from the selected informative references, "the same as

Refs. [ENI20a] and [Age20a], it is the second least linked to" the "Software inventory (AM.A)" objective of the "Asset Management" domain, and "the same as Ref. [IoT20a], it has no apparent link to" the "Hardware inventory (AM.A)" objective of the "Asset Management" domain [Pop21]. As for Refs. [Age20a] and [ENI20a], "their fairly low percentage scores are because, from the selected informative references, they are the second least linked to" both the "Hardware inventory (AM.A)" and "Software inventory (AM.B)" objectives of the "Asset Management" domain [Pop21].

Thus, based on the information disseminated by the author through the PhD report [Pop21], it is worth noting that, "among the selected informative references", Ref. [CSA19a] "is the most linked to" the "Asset Management" domain, and Ref. [IoT20a] "is the least linked to" the "Asset Management" domain [Pop21].

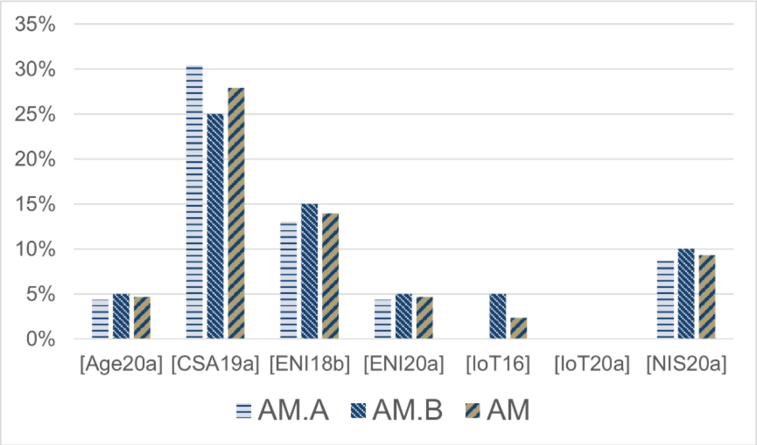


Fig. 5.5. Evaluation of selected informative references for "Asset Management" [Pop21]

5.3.3. Evaluation for Business Environment (BE)

Based on the information disseminated by the author through the PhD report [Pop21], Fig. 5.3 and 5.6 provide the percentage score for the linkage of each selected informative reference to the "Business Environment" domain of "IoTSRM2" [Pop21]. Thus, "from the selected informative references, the top three most linked to" the "Business Environment" domain are "Refs. [ENI18b], [Age20a], and [ENI20a], in that order, where both Refs. [Age20a] and [ENI20a] share the same position" [Pop21]. And, "from the selected informative references, the top three least linked to" the "Business Environment" domain are "Refs. [IoT20a], [NIS20a], and [IoT16], in that order, where both Refs. [IoT16] and [NIS20a] share the same position" [Pop21]. The rationale behind these outputs is "based on the percentage scores of the objectives corresponding to" the "Business Environment" domain of "IoTSRM2", where the "Dependencies and critical functions (BE.A)" objective "has a marginally higher number of in-scope IoT security requirements mapped to it than" the "Critical service resilience (BE.B)" objective [Pop21].

Hence, about Ref. [ENI18b], "its very high percentage score is because, from the selected informative references, it is the most linked to" both the "Dependencies and critical functions (BE.A)" and "Critical service resilience (BE.B)" objectives of the

"Business Environment" domain [Pop21]. With respect to Refs.[Age20a] and [ENI20a], even though, "from the selected informative references, Ref. [Age20a] is the third most and Ref. [ENI20a] is the second least linked to" the "Dependencies and critical functions (BE.A)" objective, they still share "the same high percentage score as Ref. [ENI20a] is the second and Ref. [Age20a] is the third most linked to" the "Critical service resilience (BE.B)" objective of the "Business Environment" domain, which makes them share the same number of in-scope IoT security requirements across the "Business Environment" domain [Pop21].

Next, with respect to Ref. [IoT20a], its very low percentage score is because, "it has no apparent link to" the "Dependencies and critical functions (BE.A)" objective, and "it is the third least linked to" the "Critical service resilience" (BE.B) objective, having a smaller number of IoT security requirements mapped to it than Refs. [IoT16] and [NIS20a] each have for the "Dependencies and critical functions" (BE.A) objective [Pop21]. About Refs. [NIS20a] and [IoT16], "their same low percentage score is because", from the selected informative references, "they have no apparent links to" the "Critical service resilience (BE.B)" objective, and "they share the position of the third least linked to" the "Dependencies and critical functions (BE.A)" objective [Pop21].

Thus, based on the information disseminated by the author through the PhD report [Pop21], it is worth noting that, "among the selected informative references", Ref. [ENI18b] "is the most linked to" the "Business Environment" domain, and Ref. [IoT20a] "is the least linked to" the "Business Environment" domain [Pop21].

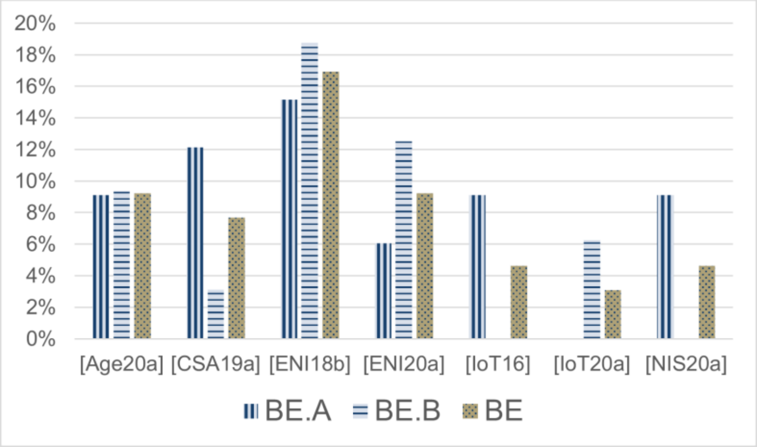


Fig. 5.6. Evaluation of selected informative references for "Business Environment" [Pop21]

5.3.4. Evaluation for Governance (GV)

Based on the information disseminated by the author through the PhD report [Pop21], Fig. 5.3 and 5.7 provide the percentage score for the linkage of each selected informative reference to the "Governance" domain of "IoTSRM2" [Pop21]. Hence, "from the selected informative references, Refs. [ENI18b], [IoT20a], and [CSA19a] resulted in being the top three most linked to" the "Governance" domain, in that order, whereas "Refs. [IoT16], [ENI20a], and [NIS20a] resulted in being the top three least linked to” the “Governance” domain, in that order [Pop21]. The rationale behind these outputs is “based on the percentage scores of the objectives corresponding to” the “Governance” domain of “IoTSRM2”, where “the greatest number of in-scope IoT security requirements are mapped to” the “Governance and risk management plans (GV.D)” objective, followed by the “Security related policies (GV.A)”, “Structures and responsibilities (GV.B)”, and “Regulatory requirements (GV.C)” objectives, in that order [Pop21]. In this context, the outputs are very much driven by the “Security related policies (GV.A)” and “Governance and risk management plans (GV.D)” objectives of “IoTSRM2” given that “the number of in-scope IoT security requirements mapped against them amount to around 86% of the total number of in-scope IoT security requirements linked to” the “Governance” domain [Pop21].

Thus, with respect to Ref. [ENI18b], “its very high percentage score is primarily because, it is very much focused on” the “Governance” domain and, “from the selected informative references, it is the most linked to” the “Governance and risk management plans (GV.D)” objective [Pop21]. About Ref. [IoT20a], “its high percentage score is mainly because”, from the selected informative references, “it is the most linked to” the “Governance and risk management plans (GV.D)” objective after Ref. [ENI18b], and “the most linked to” the “Security related policies (GV.A)” objective [Pop21]. Regarding Ref. [CSA19a], “its fairly high percentage score is mainly because, from the selected informative references, it is the third most linked to” both the “Security related policies (GV.A)” and the “Governance and risk management plans (GV.D)” objectives [Pop21].

Then, with regards to Ref. [IoT16], “its very low percentage score is largely because, from the selected informative references, it is the least linked to” both the “Security related policies (GV.A)” and the “Governance and risk management plans (GV.D)” objectives [Pop21]. About Ref. [ENI20a], “its low percentage score is mostly because, from the selected informative references, it is the second least linked to” both the “Security related policies (GV.A)” and the “Governance and risk management plans (GV.D)” objectives [Pop21]. As for Ref. [NIS20a], “its fairly low percentage score is mostly because, from the selected informative references, it is the third least linked to” both the “Security related policies (GV.A)” and the “Governance and risk management plans (GV.D)” objectives [Pop21].

Thus, based on the information disseminated by the author through the PhD report [Pop21], it is worth noting that, “among the selected informative references”, Ref. [ENI18b] “is the most linked to” the “Governance” domain, and Ref. [IoT16] “is the least linked to” the “Governance” domain [Pop21].

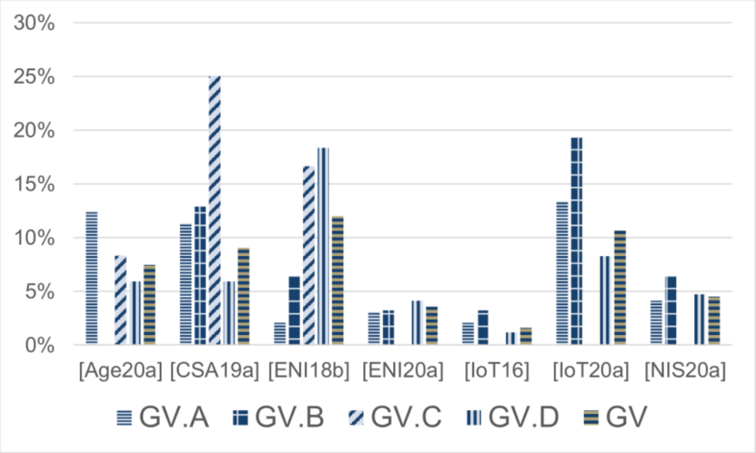


Fig. 5.7. Evaluation of selected informative references for "Governance" [Pop21]

5.3.5. Evaluation for Risk Assessment (RA)

Based on the information disseminated by the author through the PhD report [Pop21], Fig. 2.3 and 2.8 provide the percentage score for the linkage of each selected informative reference to the "Risk Assessment" domain of "IoTSRM2" [Pop21]. Thus, "from the selected informative references, the top three most linked to" the "Risk Assessment" domain are Refs. [CSA19a], [ENI18b], and [IoT16], in that order [Pop21]. In addition, "from the selected informative references, the top four least linked to" the "Risk Assessment" domain are Refs. [NIS20a], [IoT20a], [ENI20a], and [Age20a], in that order, where "both Refs. [ENI20a], and [Age20a] share the same position" [Pop21]. The rationale behind these outputs is "based on the percentage scores of the objectives corresponding to" the "Risk Assessment" domain of "IoTSRM2", where "the greatest number of in-scope IoT security requirements correspond to" the "Vulnerability discovery (RA.A)" objective, followed by the "Threat identification (RA.B)", "Risk analysis (RA.C)", and "Risk responses (RA.D)" objectives, in that order [Pop21]. In this context, the outputs are very much driven by the "Vulnerability discovery (RA.A)", "Threat identification (RA.B)", and "Risk analysis (RA.C)" objectives of "IoTSRM2" given that "the number of in-scope IoT security requirements mapped against them amount to around 88% of the total number of in-scope IoT security requirements linked to" the "Governance" domain [Pop21].

Hence, about Ref. [CSA19a], "its very high percentage score is primarily because, it is very much focused on" the "Risk Assessment" domain and, from the selected informative references, "it is the most linked to" the "Vulnerability discovery (RA.A)" objective, then, the same as Ref. [ENI18b], "it is the most linked to" the "Risk analysis (RA.C)" objective, and "it is the second most linked to" the "Threat identification (RA.B)" objective [Pop21]. About Ref. [ENI18b], "its high percentage score is mostly because", from the selected informative references, "it is the most linked to" both the "Threat identification (RA.B)" and "Risk analysis (RA.C)" objectives, and "it is the second most linked to" the "Vulnerability discovery (RA.A)" objective [Pop21]. With respect to Ref. [IoT16], "its fairly high percentage score is mostly because, it is very much focused on" the "Risk Assessment" domain and, from the selected informative references, "it is the second most linked to" the "Risk analysis (RA.C)" objective, then, "the same as Refs. [Age20a] and [ENI20a], it is the third most linked to" the "Vulnerability discovery (RA.A)" objective, and "it is the third most linked to" the "Threat identification (RA.B)" objective [Pop21].

Next, regarding Ref. [NIS20a], "its very low percentage score is mainly because, from the selected informative references, it is the least linked to" the "Vulnerability discovery (RA.A)", "Threat identification (RA.B)", and "Risk analysis (RA.C)" objectives of the "Business Environment" domain [Pop21]. With respect to Ref. [IoT20a], "its low percentage score is primarily because, from the selected informative references, it is the second least linked to" the "Vulnerability discovery (RA.A)", "Threat identification (RA.B)", and "Risk analysis (RA.C)" objectives [Pop21]. As for Refs. [ENI20a] and [Age20a], from the selected informative references, "they are the third most linked to" the "Vulnerability discovery (RA.A)" objective and "the third least linked to" the "Threat identification (RA.B)" objective [Pop21]. Moreover, even though Ref. [Age20a] "is the third most linked to" the "Risk analysis (RA.C)" objective and Ref. [ENI20a] "is the most linked to" the "Risk analysis (RA.C)" right after Ref. [Age20a], "they share the same fairly low percentage score as Ref. [ENI20a] is the third and Ref. [Age20a] is the fourth most linked to" the "Risk responses (RA.D)" objective, which "makes them share the same number of in-scope IoT security requirements across" the "Risk Assessment" domain [Pop21].

Thus, based on the information disseminated by the author through the PhD report [Pop21], it is worth noting that, "among the selected informative references", Ref. [CSA19a] "is the most linked to" the "Risk Assessment" domain, and Ref. [NIS20a] "is the least linked to" the "Risk Assessment" domain [Pop21].

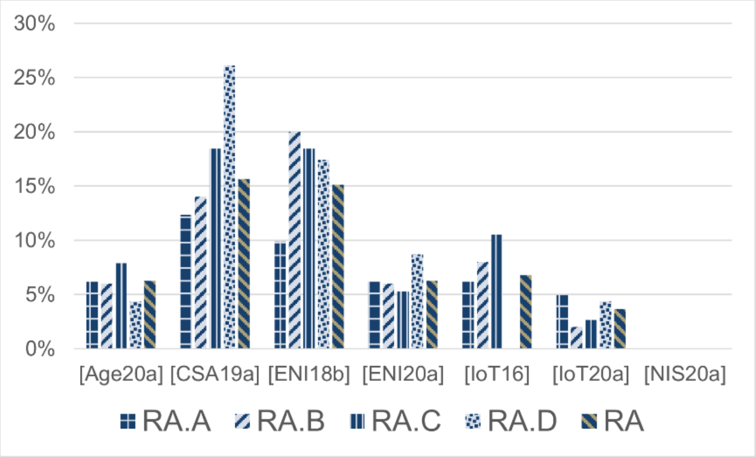


Fig. 5.8. Evaluation of selected informative references for "Risk Assessment" [Pop21]

5.3.6. Evaluation for Risk Management Strategy (RM)

Based on the information disseminated by the author through the PhD report [Pop21], Fig. 5.3 and 5.9 provide the percentage score for the linkage of each selected informative reference to the "Risk Management Strategy" domain of "IoTSRM2"

[Pop21]. Thus, "from the selected informative references, the top three most linked to" the "Risk Management Strategy" domain are Refs. [CSA19a], [ENI18b], and [IoT20a], where "they all share the same position" [Pop21]. And, "from the selected informative references, the top three least linked to" the "Risk Management Strategy" domain are Refs. [IoT16], [ENI20a], and [Age20a], where "they all share the same position" [Pop21]. The rationale behind these outputs is "based on the percentage scores of the objectives corresponding to" the "Risk Management Strategy" domain of "IoTSRM2", where the "Risk appetite and tolerances (RM.A)" objective "has the same number of in-scope IoT security requirements mapped to it" as the "Context-informed risk tolerances (RM.B)" objective [Pop21].

Hence, about Refs. [CSA19a], [ENI18b], and [IoT20a], "their very high percentage score is because, from the selected informative references, they are the most linked to" both the "Risk appetite and tolerances (RM.A)" and "Context-informed risk tolerances (RM.B)" objectives [Pop21].

Then, about Refs. [IoT16], [ENI20a], and [Age20a], "their very low percentage score is because, from the selected informative references, they are the least linked to" the both the "Risk appetite and tolerances (RM.A)" and "Context-informed risk tolerances (RM.B)" objectives [Pop21].

Thus, based on the information disseminated by the author through the PhD report [Pop21], it is worth noting that, "among the selected informative references", Refs. [CSA19a], [ENI18b], and [IoT20a] "are the most linked to" the "Risk Management Strategy" domain, and Refs. [IoT16], [ENI20a], and [Age20a] "are the least linked to" the "Risk Management Strategy" domain [Pop21].

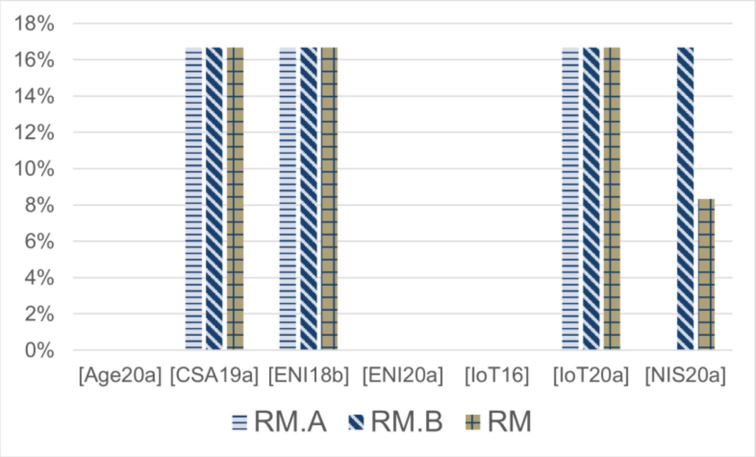


Fig. 5.9. Evaluation of selected informative references for "Risk Management Strategy" [Pop21]

5.3.7. Evaluation for Supply Chain Risk Management (SC)

Based on the information disseminated by the author through the PhD report [Pop21], Fig. 5.3 and 5.10 provide the percentage score for the linkage of each selected informative reference to the "Supply Chain Risk Management" domain of "IoTSRM2" [Pop21]. Thus, "from the selected informative references, the top three most linked to" the "Supply Chain Risk Management" domain are Refs. [Age20a], [ENI18b], and [CSA19a], in that order [Pop21]. In addition, "from the selected informative references, the top three least linked to" the "Supply Chain Risk Management" domain are Refs. [IoT20a], [IoT16], and [NIS20a], in that order, where both Refs. [IoT20a] and [IoT16] "share the same position" [Pop21]. The rationale behind these outputs is "based on the percentage scores of the objectives corresponding to" the "Supply Chain Risk Management" domain of "IoTSRM2", where the "Supplier contract management (SC.B)" objective "has a higher number of in-scope IoT security requirements mapped to it than" the "Supplier assessment (SC.A)" objective [Pop21].

In this context, the outputs are driven by the "Supplier contract management (SC.B)" given that "the number of in-scope IoT security requirements mapped against it amounts to around 62% of the total number of in-scope IoT security requirements linked to" the "Supply Chain Risk Management" domain [Pop21]. Hence, about Ref. [Age20a], "its very high percentage score is mostly because, from the selected informative references, it is the most linked to" the "Supplier contract management (SC.B)" objective [Pop21]. With regards to Ref. [ENI18b], "its high percentage score is because", from the selected informative references, "it is the second most linked to" the "Supplier contract management (SC.B)" objective, and "it is the most linked to" the "Supplier assessment (SC.A)" objective [Pop21]. About Ref. [CSA19a], "its fairly high percentage score is because, from the selected informative references, it is the third most linked to" both the "Supplier assessment (SC.A)" and "Supplier contract management (SC.B)" objectives [Pop21].

Next, with respect to Refs. [IoT20a] and [IoT16], "their same very low percentage score is mostly because, from the selected informative references, they are the least and second least linked to" the "Supplier contract management (SC.B)" objective, respectively [Pop21]. As for Ref. [NIS20a], "its low percentage score is because", from the selected informative references, "it is the third least linked to" the "Supplier contract management (SC.B)" objective, and, "the same as Ref. [IoT20a], it is the second least linked to" the "Supplier assessment (SC.A)" objective [Pop21].

Thus, based on the information disseminated by the author through the PhD report [Pop21], it is worth noting that, "among the selected informative references", Ref. [Age20a] "is the most linked to" the "Supply Chain Risk Management" domain, and Refs. [IoT20a] and [IoT16] "are the least linked to" the "Supply Chain Risk Management" domain [Pop21].

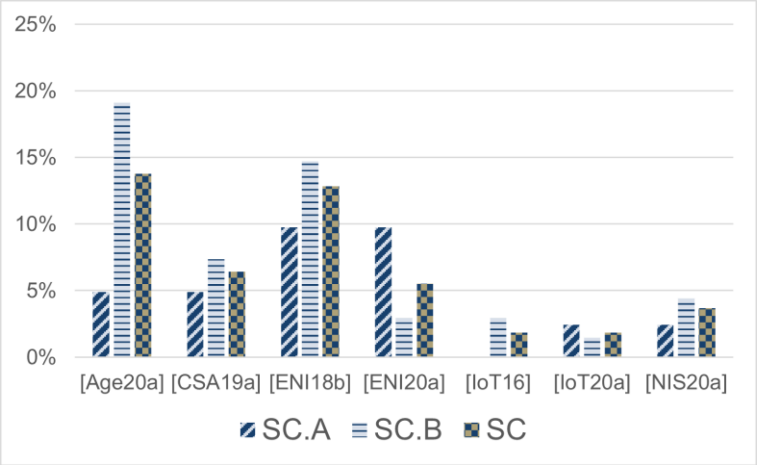


Fig. 5.10. Evaluation of selected informative references for "Supply Chain Risk Management" [Pop21]

5.4. Related Work

Based on the information disseminated by the author through the research paper [Pop+21a], "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., [CSD19], [ETS20], [BIT16], [Liu+17], [R+18]) [Pop+21a]. Moreover, "at the time of writing, there is no research article nor best practice to exclusively focus on IoT security risk management strategy" [Pop+21a]. In this context, Lee (2020) [Lee20] 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" [Pop+21a]. Nevertheless, "the IoT cyber risk management framework proposed by Lee (2020) [Lee20] 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" [Pop+21a]. Thus, compared with the work performed by Lee (2020) [Lee20], "the 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" [Pop+21a].

Furthermore, „the available documentation around the 25 selected IoT security best practices was used to provide the proposed IoTSRM2 and the analysis of IoTSRM2's related work" from this subchapter (see Table 5.24) [Pop+21a].

Then, based on the information disseminated by the author through the research paper [Pop+21a], "with respect to the analysis of IoTSRM2's related work", Table 5.24 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" [Pop+21a]. With respect to the proposed evaluation criteria, "eight evaluation criteria were formulated based on the proposed methodology for developing the IoTSRM2" [Pop+21a] (see Chapter 5.1). Also, 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" [Pop+21a].

Table 5.24. IoTSRM2 and related work mapped to evaluation criteria and extent of applicability [Pop+21a]

	Extent of Applicability		
Evaluation Criterion	**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" [Pop+21a]	[Age20a], [DHS16], [ENI20a], [IoT16], [NEM18], [NIS20a], [OTA18], IoTSRM2	[Com20], [CSA15], [CSA16], [DCM18a], [ENI17b], [ENI18b], [ENI19b], [ENI20b], [IIC16], [NHT16]	[AIO16], [BIT16], [CSA19a], [CSD19], [ETS20], [GSM18], [IEE17], [IoT20a]
"E2: Methodology for developing the recommended IoT security requirements / controls is clearly described" [Pop+21a]	[AIO16], [CSD19], [ENI17b], [ENI18b], [ENI19b], [ENI20a], [ENI20b], IoTSRM2	[Age20a], [BIT16], [DCM18a], [ETS20]	[Com20], [CSA15], [CSA16], [CSA19a], [DHS16], [GSM18], [IEE17], [IIC16], [IoT16], [IoT20a], [NEM18], [NHT16], [NIS20a], [OTA18]
"E3: Mapping of IoT security requirements / controls to NIST CSF's Categories and Subcategories" [Pop+21a]	"IoTSRM2, but none of the 25 selected IoT security best practices"	[Age20a], [ENI17b]	"All 25 selected IoT security best practices except" [Age20a], [ENI17b]
"E4: Clearly indicate for each IoT security requirement / control expected IoT security actions / activities from IoT suppliers of the target audience" [Pop+21a]	"IoTSRM2, but none of the 25 selected IoT security best practices"	[BIT16], [CSA15], [DHS16], [ENI17b], [ENI18b], [ENI19b], [ENI20a], [ENI20b], [IIC16], [IoT16]	[Age20a], [AIO16], [Com20], [CSA16], [CSA19a], [CSD19], [DCM18a], [ETS20], [GSM18], [IEE17], [IoT20a], [NEM18], [NHT16], [NIS20a], [OTA18]
"E5: Provides integration points with the cybersecurity program as part of each IoT security requirement / control" [Pop+21a]	"IoTSRM2, but none of the 25 selected IoT security best practices"	[CSA16], [ENI18b], [ENI19b], [ENI20a]	"All 25 selected IoT security best practices except" [CSA16], [ENI18b], [ENI19b], [ENI20a]
"E6: Mapping of relevant IoT security best practices with unique identifiers to each recommended	[CSD19], [DCM18a], "IoTSRM2"	[Age20a], [CSA19a], [ENI17b], [ENI18b], [ENI19b], [ENI20b], [IoT16], [IoT20a],	[AIO16], [BIT16], [Com20], [CSA15], [CSA16], [DHS16], [ENI20a], [ETS20],

	Extent of Applicability		
Evaluation Criterion	**The Evaluation Criterion Fully Applies**	**The Evaluation Criterion Applies to a Certain Extent, but not Fully**	**The "as-is" Evaluation Criterion Does Not Apply**
IoT security requirement / control" [Pop+21a]		[NEM18], [NHT16], [NIS20a]	[GSM18], [IEE17], [IIC16], [OTA18]
"E7: Prioritization of the recommended IoT security requirements / controls" [Pop+21a]	[Com20], [DCM18a], [IEE17], "IoTSRM2"	[Age20a], [GSM18], [IoT20a], [OTA18]	"All 25 selected IoT security best practices except" [Age20a], [Com20], [DCM18a], [GSM18], [IEE17], [IoT20a], [OTA18]
"E8: Provides statistics for the mapping of informative references" [Pop+21a]	[DCM18a], "IoTSRM2"	"None of the 25 selected IoT security best practices"	"All 25 selected IoT security best practices except" [DCM18a]

Following Table 5.24, based on the information disseminated by the author through the research paper [Pop+21a], this subchapter "presents the evaluation of IoTSRM2 and the 25 selected IoT security best practices for each evaluation criterion" [Pop+21a].

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

Based on the information disseminated by the author through the research paper [Pop+21a], "the proposed IoTSRM2 is exclusively focused on IoT security risk management strategy" [Pop+21a]. And, "from the 25 selected IoT security best practices, seven of them focused on strategic IoT security activities (i.e., [Age20a], [DHS16], [ENI20a], [IoT16], [NEM18], [NIS20a], [OTA18]), ten of them had a partial focus on strategic IoT security activities (i.e., [Com20], [CSA15], [CSA16], [DCM18a], [ENI17b], [ENI18b], [ENI19b], [ENI20b], [IIC16], [NHT16]), while the remaining ones focused on technical IoT security activities (i.e., [AIO16], [BIT16], [CSA19a], [CSD19], [ETS20], [GSM18], [IEE17], [IoT20a])" [Pop+21a].

"Regarding the seven selected IoT security best practices that focused on strategic IoT security activities", AgeLight LLC (2020a) [Age20a], DHS (2016) [DHS16], NEMA (2018) [NEM18], and OTA (2018) [OTA18] "provided strategic IoT security principles", ENISA (2020a) [ENI20a] "provided strategic guidelines specifically focused on procurement in hospitals", IoTAC (2016) [IoT16] "provided basic strategic guidance for providers and users of IoT devices, systems, and services across industries", and NIST (2020a) [NIS20a] "provided premarket and postmarket cybersecurity activities with a strategic focus for IoT device manufacturers" [Pop+21a]. Similar to these seven selected IoT security best practices which "provided IoT security requirements with a strategic focus", the proposed "IoTSRM2" provides "domains, objectives, and controls focused on strategic IoT security practices" [Pop+21a]. Notwithstanding, compared with the seven selected IoT security best practices which "were not exclusively focused on IoT security risk management strategy", this thesis "proposes a reference model for IoT security risk management strategy (i.e., IoTSRM2) applicable to IoT adopters from any sector" [Pop+21a].

Furthermore, "from the perspective of the extent of applicability to this evaluation criterion", compared with the ten selected IoT security best practices (i.e., [Com20], [CSA15], [CSA16], [DCM18a], [ENI17b], [ENI18b], [ENI19b], [ENI20b], [IIC16], [NHT16]) which "besides the strategic IoT security practices focused on some technical IoT security practices", the proposed "IoTSRM2" exclusively focused on "strategic IoT security practices" [Pop+21a].

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

Based on the information disseminated by the author through the research paper [Pop+21a], "the proposed methodology for developing IoTSRM2 controls is clearly described" [Pop+21a]. And, "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., [AIO16], [CSD19], [ENI17b], [ENI18b], [ENI19b], [ENI20a], [ENI20b]), four of them partially described their methodology (i.e., [Age20a], [BIT16], [DCM18a], [ETS20]), while the remaining ones have not described their methodology (i.e., [Com20], [CSA15], [CSA16], [CSA19a], [DHS16], [GSM18], [IEE17], [IIC16], [IoT16], [IoT20a], [NEM18], [NHT16], [NIS20a], [OTA18])" [Pop+21a].

"Regarding the seven selected IoT security best practices that clearly described their methodologies", AIOTI (2016) [AIO16] "provided details about the aspects discussed as part of the four sessions workshop", CSDE (2019) [CSD19] "developed the IoT security requirements by identifying common IoT security device capabilities from Convening the Conveners (C2) organizations", ENISA (2020a) [ENI20a] "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., [ENI17b], [ENI18b], [ENI19b], [ENI20b]) "used the ENISA's five-step methodology involving both desktop research and interviews" [Pop+21a]. Compared with the high-level five-step methodology from ENISA (i.e., [ENI17b], [ENI18b], [ENI19b], [ENI20b]), "the 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" [Pop+21a]. Even though the proposed methodology from this chapter has different objectives than the studies conducted by ENISA (2017b,2018b, 2019b, 2020b), "similar to the methodology of ENISA (i.e., [ENI17b], [ENI18b], [ENI19b], [ENI20b]) which included scope definition, desktop research, and analysis and development tasks, among others, the proposed methodology for developing the IoTSRM2 includes several steps related to scoping, analysis, and creation phases that involve extensive research work" [Pop+21a]. In addition, "in contrast to the research works performed by AIOTI (2016) [AIO16], CSDE (2019) [CSD19], and ENISA (2020a) [ENI20a] which are limited to workshops, surveys, and interviews, respectively, the proposed methodology from this chapter is based on selected IoT security best practices" [Pop+21a].

Furthermore, "from the perspective of the extent of applicability to this evaluation criterion, the proposed methodology for developing the IoTSRM2 differentiates from the methodologies provided by AgeLight LLC (2020a) [Age20a], BITAG (2016) [BIT16], DCMS (2018a) [DCM18a], and ETSI (2020) [ETS20] as it is much more detailed than the ones of the four selected IoT security best practices which offered limited details" [Pop+21a]. Thus, first AgeLight LLC (2020a, 2020b) [Age20a], [Age20b] "developed the recommended IoT security requirements based on seven pre-established guiding tenets and dozens of industry and governmental efforts"

[Pop+21a]. Notwithstanding, AgeLight LLC (2020a, 2020b) [Age20a], [Age20b] "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" [Pop+21a]. Second, BITAG (2016) [BIT16] "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" [Pop+21a]. Then, DCMS (2018a, 2018b) [DCM18a], [DCM18b] "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 [DCM18b]" [Pop+21a]. As for ETSI (2020) [ETS20], 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" [Pop+21a].

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

As per Table 5.24 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" [Pop+21a]. However, AgeLight LLC (2020a) [Age20a] and ENISA (2017b) [ENI17b] "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" [Pop+21a]. "In contrast to the 25 selected IoT security best practices", the 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 Chapters 5.1 and 5.2) [Pop+21a].

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

Based on the information disseminated by the author through the research paper [Pop+21a], "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" [Pop+21a]. However, ten of these, namely BITAG (2016) [BIT16], CSA (2015) [CSA15], DHS (2016) [DHS16], ENISA (2017b) [ENI17b], ENISA (2018b) [ENI18b], ENISA (2019b) [ENI19b], ENISA (2020a) [ENI20a], ENISA (2020b) [ENI20b], IIC (2016) [IIC16], and IoTAC (2016) [IoT16], "indicated for some IoT security requirements expected IoT security actions / activities from IoT suppliers of the target audience" [Pop+21a]. "In contrast to the 25 selected IoT security best practices", the 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" [Pop+21a].

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

Based on the information disseminated by the author through the research paper [Pop+21a], "none of the 25 selected IoT security best practices provided integration points with the cybersecurity program as part of each IoT security requirement" [Pop+21a]. Notwithstanding, CSA (2016) [CSA16], ENISA (2018b) [ENI18b], ENISA (2019b) [ENI19b], and ENISA (2020a) [ENI20a] "provided for a few IoT security requirements integration points with the cybersecurity program"

[Pop+21a]. "Compared with the 25 selected IoT security best practices", the 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" [Pop+21a].

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

Based on the information disseminated by the author through the research paper [Pop+21a], "the proposed methodology for developing IoTSRM2 involves the mapping of the 25 selected IoT security best practices with unique identifiers to each IoTSRM2 control where applicable" [Pop+21a]. And, "from the 25 selected IoT security best practices, two of them provided the mapping of relevant IoT security best practices with unique identifiers to each recommended IoT security requirement (i.e., [CSD19], [DCM18a]), eleven of them partially provided this type of mapping (i.e., [Age20a], [CSA19a], [ENI17b], [ENI18b], [ENI19b], [ENI20b], [IoT16], [IoT20a], [NEM18], [NHT16], [NIS20a]), while the remaining ones have not provided this type of mapping (i.e., [AIO16], [BIT16], [Com20], [CSA15], [CSA16], [DHS16], [ENI20a], [ETS20], [GSM18], [IEE17], [IIC16], [OTA18])" [Pop+21a].

"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 (2019) [CSD19] "provided under individual annexes the mapping of each IoT security requirement to the applicable requirement(s) of eleven best practices", and DCMS (2018a) [DCM18a] "provided in a separate document (i.e., [DCM18b]) the mapping of IoT security recommendations, guidance and standards to each IoT security requirement of its code of practice" [Pop+21a]. In this context, "the mapping from IoTSRM2 is similar to the mappings provided by CSDE (2019) [CSD19] and DCMS (2018a, 2018b) [DCM18a], [DCM18b] which also provided the applicable informative references with associated unique identifiers (UIDs) of the in-scope IoT security requirements from various selected best practices" [Pop+21a]. In addition, CSDE (2019) [CSD19] and DCMS (2018a, 2018b) [DCM18a], [DCM18b] "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" [Pop+21a].

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" [Pop+21a]. Thus, first AgeLight LLC (2020a) [Age20a], ENISA (2017b) [ENI17b], ENISA (2018b) [ENI18b], ENISA (2019b) [ENI19b] and ENISA (2020b) [ENI20b] "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" [Pop+21a]. Second, IoTAC (2016) [IoT16], NHTSA (2016) [NHT16] and NIST (2020a) [NIS20a] "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" [Pop+21a]. Then, NEMA (2018) [NEM18] "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" [Pop+21a]. Further, IoTSF (2020a, 2020b) [IoT20a], [IoT20b] "provided the mapping of framework sections to ETSI TS 103 645 as part of the IoTSF Compliance Questionnaire [IoT20b], but this mapping was limited to framework sections rather than recommended IoT security requirements"

[Pop+21a]. And CSA (2019a) [CSA19a] "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" [Pop+21a].

"E7: Prioritization of the recommended IoT security requirements / controls"

Based on the information disseminated by the author through the research paper [Pop+21a], "the proposed IoTSRM2 provides prioritized IoTSRM2 controls" [Pop+21a]. And, "from the 25 selected IoT security best practices, three of them provided the prioritization of the recommended IoT security requirements (i.e., [Com20], [DCM18a], [IEE17]), four of them partially provided the prioritization of the recommended IoT security requirements (i.e., [Age20a], [GSM18], [IoT20a], [OTA18]), while the remaining ones did not provide this prioritization" [Pop+21a].

"Regarding the three selected IoT security best practices that provided the prioritization of the recommended IoT security requirements", Commonwealth of Australia (2020) [Com20] and DCMS (2018a) [DCM18a] "prioritized their IoT security requirements recommending industry to prioritize the top three in the short-term" and IEEE (2017) [IEE17] "prioritized its eleven IoT security requirements based on their relevance to IoT" [Pop+21a]. "Similar to these three IoT security best practices", the proposed "IoTSRM2" provides "prioritized IoTSRM2 controls" [Pop+21a]. However, "compared with these IoT security best practices which provided the prioritization of their IoT security requirements without describing how their prioritization resulted, the proposed methodology for developing the IoTSRM2 outlines the way in which the prioritization of IoTSRM2 controls for each IoTSRM2 objective was made" [Pop+21a]. In addition, the proposed "IoTSRM2" provides "the prioritization of IoTSRM2 domains based on the number of IoTSRM2 objectives corresponding to each IoTSRM2 domain" [Pop+21a].

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" [Pop+21a]. Thus, first AgeLight LLC (2020a) [Age20a] "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 & costs, regulatory risk)" [Pop+21a]. Second, GSM Association (2018) [GSM18] "prioritized only some IoT security requirements as Critical, High, Medium and Low instead of prioritizing all recommended IoT security requirements" [Pop+21a]. Then, IoTSF (2020a) [IoT20a] "classified each IoT security requirement as Mandatory or Advisory rather than providing a comprehensive prioritization of its recommended IoT security requirements" [Pop+21a]. Further, OTA (2018) [OTA18] "classified each IoT security requirement as Required (Must) or Recommended (Should) instead of providing a comprehensive prioritization of its recommended IoT security requirements" [Pop+21a].

"E8: Provides statistics for the mapping of informative references"

Based on the information disseminated by the author through the research paper [Pop+21a], "the proposed IoTSRM2 provides statistics for the mapping of informative references" [Pop+21a]. And, "from the 25 selected IoT security best practices, only DCMS (2018a) [DCM18a] provided statistics for the mapping of informative references to their recommended best practices, while the remaining ones did not provide any statistics" [Pop+21a]. "Similar to DCMS (2018a) [DCM18a] which provided the total number of IoT security recommendations mapped for each informative reference", the proposed "IoTSRM2" provides, "for each informative reference of IoTSRM2, the total number of unique in-scope IoT security requirements mapped to IoTSRM2 controls" [Pop+21a].

5.5. Conclusions

This chapter extended the research work on the IoT security best practices outlined in Chapter 2 by proposing a methodology for developing the IoT security risk management strategy reference model, developing the proposed "IoT security risk management strategy reference model (IoTSRM2)", critically evaluating selected informative references, and providing a comprehensive analysis of the related work for the "IoTSRM2" based on eight evaluation criteria. Thus, by addressing the need for a reference model for IoT security risk management strategy, this chapter aimed 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 chapter described the 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 chapter 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, this chapter presented the proposed "IoTSRM2" which consists of 6 domains, 16 objectives, and 30 controls for IoT adopters from any sector, which should be addressed by both IoT adopters and IoT suppliers. First, this chapter provided an illustrative overview of the proposed "IoTSRM2". Then, for each informative reference of the proposed "IoTSRM2", this chapter provided the total number of unique in-scope IoT security requirements mapped to the "IoTSRM2" controls, and it indicated whether the informative reference resulted in being among the informative references that are the most relevant to IoT security risk management strategy. Next, for each "IoTSRM2" domain, this chapter provided the "IoTSRM2" objectives, and, for each "IoTSRM2" objective, it described the "IoTSRM2" controls in line with the target information granularity, and it provided, among others, the prioritization of "IoTSRM2" controls based on their adjusted weights.

Afterwards, this chapter provided the critical evaluation of selected informative references of "IoTSRM2" based on their percentage-wise linkage to "IoTSRM2", and was structured in seven parts, namely in the overall evaluation of selected informative references and the individual evaluations of selected informative references for each IoTSRM2 domain. In this respect, from the 25 informative references of "IoTSRM2", seven informative references (i.e., Refs. [Age20a], [CSA19a], [ENI18b], [ENI20a], [IoT16], [IoT20a], and [NIS20a]) were selected for the evaluation as these resulted in being the most relevant to IoT security risk management strategy based on the fulfilment of the two inclusion criteria and two conditions. Hence, with respect to "the overall evaluation of selected informative references", for instance, the findings revealed that Ref. [ENI18b] has the strongest links to "IoTSRM2" among all 25 informative references and that Ref. [IoT16] is the least linked to "IoTSRM2" among the selected informative references. Moreover, among others, the findings revealed that the majority of the selected informative references are the most focused on the "Governance" domain, and they are the least focused on the "Risk Management Strategy" domain.

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

Furthermore, this chapter 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 chapter 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 (i.e., "the evaluation criterion fully applies", "the evaluation criterion applies to a certain extent, but not fully", and "the as-is evaluation criterion does not apply").

This chapter provided the following contributions:

- The design of a methodology for developing the IoT security risk management strategy reference model based on best practices;
- The development of a reference model for IoT security risk management strategy that is suitable for IoT adopters from any sector based on the proposed methodology;
- A critical evaluation of selected informative references of the IoTSRM2 based on their linkage to the proposed reference model;
- A comparative analysis of the related work for the proposed reference model based on a proposed set of evaluation criteria.

6. APPLICATION OF AN IoTSRM2-BASED SURVEY

Based on the information disseminated by the author through the research paper [Pop+21b] and the PhD report [Pop21], this chapter extends on Chapter 5 and focuses on addressing "the undertaking of an IoTSRM2-based survey to determine the current state of IoT security risk management strategies in surveyed organizations relative to IoTSRM2" [Pop+21b]. Moreover, considering that, "at the time of writing, there is no research study found to exclusively focus on determining the current state of IoT security risk management strategies in surveyed organizations, there is a clear research gap in terms of the existence of such a research study" [Pop+21b]. Thus, the purpose of this chapter is "to undertake an IoTSRM2-based survey to determine the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2 considering the views of leaders from industries and governments from around the world" [Pop+21b]. Moreover, this chapter aims "to support IoT security practitioners from industries and governments to establish the current state of their IoT security risk management strategies when benchmarked against their peers and in turn to enable them to enhance these strategies for matching or outrunning the IoT security risk management strategies of their peers" [Pop+21b].

First, this chapter provides the research questions of this study. Second, the chapter describes "the proposed three-phased methodology for addressing the research questions of this study and in turn for determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2" [Pop+21b]. Third, the chapter presents "the IoTSRM2-based survey results" [Pop+21b]. Then, the chapter presents the related work. Finally, the chapter presents the concluding remarks.

Thus, this chapter addresses the following thesis objective:

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

6.1. The Research Questions of the IoTSRM2-Based Survey Study

Based on the information disseminated by the author through the research paper [Pop+21b] and in response to the research gap and the purpose mentioned above, the research questions of this research study are the following [Pop+21b]:

- **"RQ1":** "What is the overall tendency of the IoT security risk management strategies of the surveyed organizations to meet or deviate from the IoTSRM2 controls?"

- **"RQ2":** "What is the IoTSRM2 compliance score of each of the surveyed organizations?"
- **"RQ3":** "Which is the top organization type for the surveyed organizations by survey respondents?"
- **"RQ4.a":** "Which is the top industry sector for the surveyed organizations by survey respondents?"
- **"RQ4.b":** "Which is the top industry sector for the surveyed organizations of the top organization type by survey respondents?"
- **"RQ5.a":** "What is the overall average IoTSRM2 compliance score of the surveyed organizations for each IoTSRM2 control?"
- **"RQ5.b":** "What is the overall average IoTSRM2 compliance score of the surveyed organizations of the top organization type for each IoTSRM2 control?"
- **"RQ5.c":** "What is the overall average IoTSRM2 compliance score of the surveyed organizations from the top industry sector of the top organization type for each IoTSRM2 control?"
- **"RQ6.a":** "Which is the top position level of the survey respondents for the surveyed organizations by survey respondents?"
- **"RQ6.b":** "Which is the top position level of the survey respondents for the surveyed organizations of the top organization type by survey respondents?"
- **"RQ6.c":** "Which is the top position level of the survey respondents for the surveyed organizations from the top industry sector of the top organization type by survey respondents?"
- **"RQ7.a":** "Which is the top region for the surveyed organizations by survey respondents?"
- **"RQ7.b":** "Which is the top region for the surveyed organizations of the top organization type by survey respondents?"
- **"RQ7.c":** "Which is the top region for the surveyed organizations from the top industry sector of the top organization type by survey respondents?"

Then, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.1 "provides a reading map for the above research questions" [Pop+21b]. "This mapping should be leveraged in conjunction with the 14 research questions by readers interested in specific research questions of this study" [Pop+21b], where:

- "Mapping 1 and Mapping 2 correspond to the results chapters related to the surveyed large and small-medium organizations" [Pop+21b];
- "Mapping 3, Mapping 4, and Mapping 5 correspond to the results chapters related to the surveyed large organizations, where Mapping 5 corresponds to the surveyed large organizations that operate in the Technology, Media, & Telecom (TMT) industry sector in particular" [Pop+21b].

For instance, "assuming a reader is interested in RQ3, Fig. 6.1 guides the reader via Mapping 1 to read Chapters 6.1, 6.2, 6.3.1, 6.4, and 6.5" [Pop+21b].

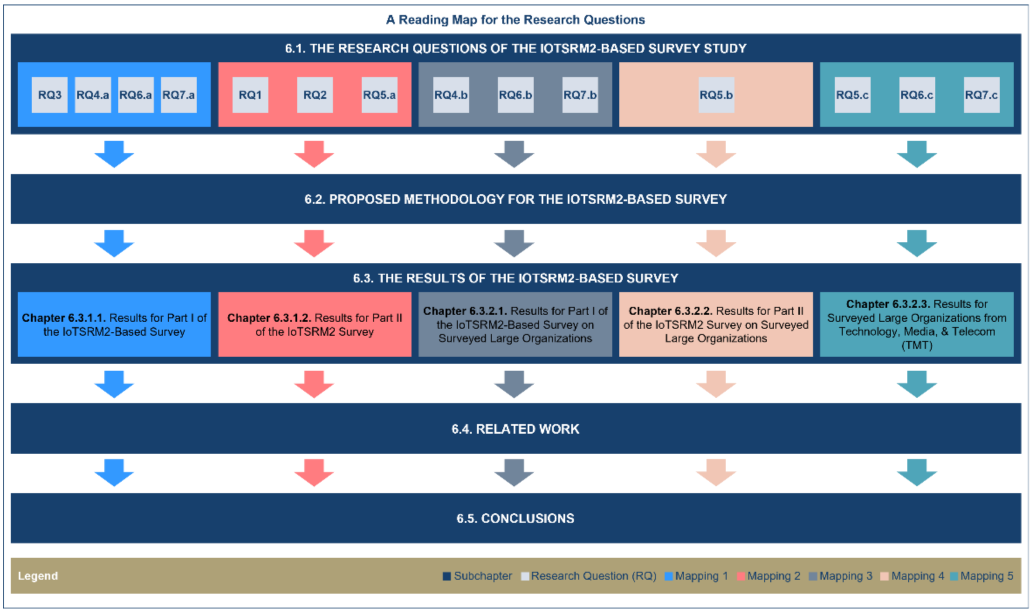

A Reading Map for the Research Questions
6.1. THE RESEARCH QUESTIONS OF THE IOTSRM2-BASED SURVEY STUDY
RQ3
RQ4.a
RQ6.a
RQ7.a
RQ1
RQ2
RQ5.a
RQ4.b
RQ6.b
RQ7.b
RQ5.b
RQ5.c
RQ6.c
RQ7.c
6.2. PROPOSED METHODOLOGY FOR THE IOTSRM2-BASED SURVEY
6.3. THE RESULTS OF THE IOTSRM2-BASED SURVEY
Chapter 6.3.1.1. Results for Part I of the IoTSRM2-Based Survey
Chapter 6.3.1.2. Results for Part II of the IoTSRM2 Survey
Chapter 6.3.2.1. Results for Part I of the IoTSRM2-Based Survey on Surveyed Large Organizations
Chapter 6.3.2.2. Results for Part II of the IoTSRM2 Survey on Surveyed Large Organizations
Chapter 6.3.2.3. Results for Surveyed Large Organizations from Technology, Media, & Telecom (TMT)
6.4. RELATED WORK
6.5. CONCLUSIONS
Legend
Subchapter
Research Question (RQ)
Mapping 1
Mapping 2
Mapping 3
Mapping 4
Mapping 5

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

6.2. Proposed Methodology for the IoTSRM2-Based Survey

Based on the information disseminated by the author through the research paper [Pop+21b], this subchapter describes "the methodology used for addressing the research questions of this survey study and in turn for achieving the intended purpose of determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoT Security Risk Management Strategy Reference Model (IoTSRM2)" [Pop+21b]. Fig. 6.2 shows "the proposed three-phased survey methodology that consists of nine steps and outputs, namely three steps with associated outputs for each of three phases (i.e., the Plan and Create, Launch and Run, and Analyze and Report phases)" [Pop+21b].

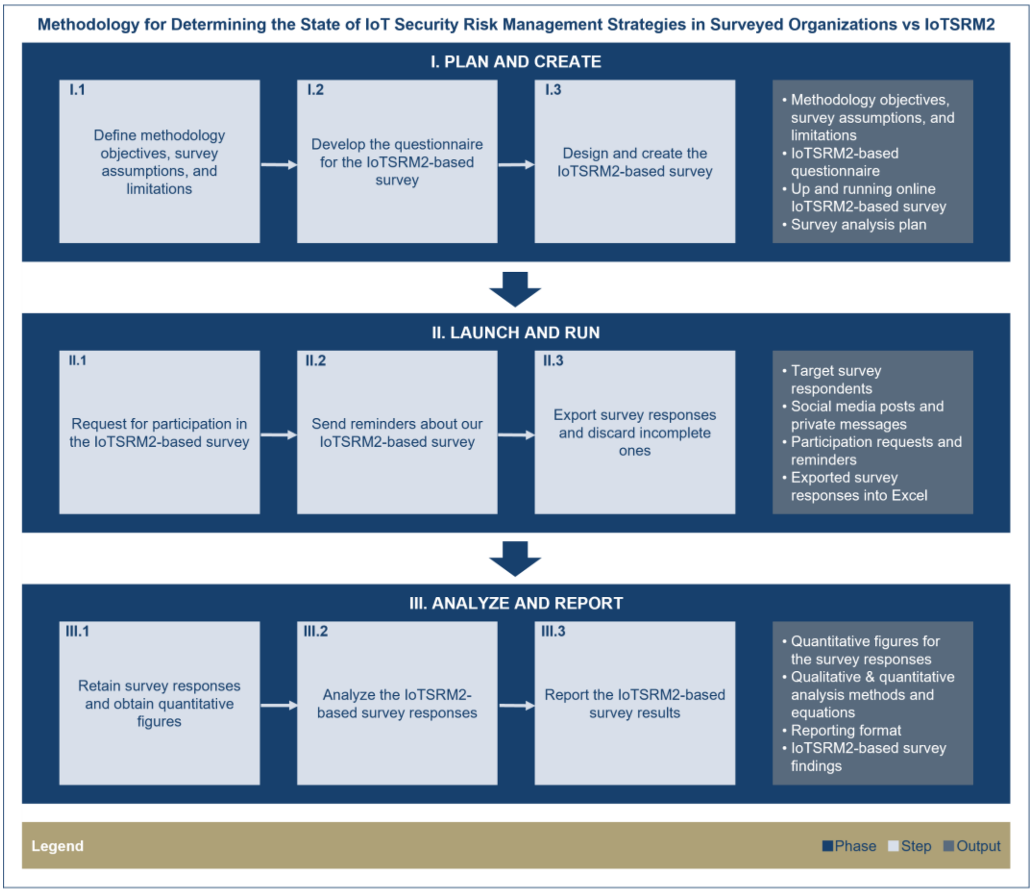

Methodology for Determining the State of IoT Security Risk Management Strategies in Surveyed Organizations vs IoTSRM2
I. PLAN AND CREATE
I.1
Define methodology objectives, survey assumptions, and limitations
I.2
Develop the questionnaire for the IoTSRM2-based survey
I.3
Design and create the IoTSRM2-based survey
• Methodology objectives, survey assumptions, and limitations
• IoTSRM2-based questionnaire
• Up and running online IoTSRM2-based survey
• Survey analysis plan
II. LAUNCH AND RUN
II.1
Request for participation in the IoTSRM2-based survey
II.2
Send reminders about our IoTSRM2-based survey
II.3
Export survey responses and discard incomplete ones
• Target survey respondents
• Social media posts and private messages
• Participation requests and reminders
• Exported survey responses into Excel
III. ANALYZE AND REPORT
III.1
Retain survey responses and obtain quantitative figures
III.2
Analyze the IoTSRM2-based survey responses
III.3
Report the IoTSRM2-based survey results
• Quantitative figures for the survey responses
• Qualitative & quantitative analysis methods and equations
• Reporting format
• IoTSRM2-based survey findings
Legend
■Phase □Step ■Output

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

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], each of the three phases of the proposed methodology together with its corresponding steps are described below [Pop+21b].

6.2.1. Phase I: Plan and Create

Based on the information disseminated by the author through the research paper [Pop+21b], the "Plan and Create" phase involves "the definition of methodology objectives, survey assumptions, and limitations (Step I.1), the development of the questionnaire for the IoTSRM2-based survey (Step I.2), and the design and creation of the IoTSRM2-based survey (Step I.3)" [Pop+21b].

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

First, based on the information disseminated by the author through the research paper [Pop+21b], "this step outlines the twelve objectives of the proposed methodology" [Pop+21b]. Thus, the main objective of the proposed methodology is:

- **"Objective 6.1"**: "Run an online anonymous survey for four weeks based on the web survey design principles [Dil+99] and IoT Security Risk Management Strategy Reference Model (IoTSRM2) (see Chapter 5.2) targeting leaders with stake in IoT security risk management strategies from industries and governments from around the world to determine the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2" [Pop+21b].

Then, the secondary objectives of the proposed methodology are:

- **"Objective 6.2"**: "Identify target groups of survey respondents to get the views of leaders from industries and governments on the IoT security risk management strategies of their organizations or client organizations relative to the IoTSRM2" [Pop+21b];
- **"Objective 6.3"**: "Organize the questionnaire of the IoTSRM2-based survey in two parts, including screening and background questions for part I of and IoTSRM2-related questions for part II of the IoTSRM2-based survey" [Pop+21b];
- **"Objective 6.4"**: "For part I of the IoTSRM2-based survey, formulate the screening and background questions with associated answer choices for each question to allow filtering and anonymous profiling of survey respondents and surveyed organizations" [Pop+21b];
- **"Objective 6.5"**: "For part II of the IoTSRM2-based survey, formulate one IoTSRM2-related question with associated answer choices for each of the 30 IoTSRM2 controls (see Chapter 5.2), to allow the determination of the current state of IoT security risk management strategies in the surveyed organizations based on IoTSRM2" [Pop+21b];
- **"Objective 6.6"**: "Identify the principles for designing web questionnaires [Dil+99], that are applicable to the IoTSRM2-based survey to allow its corresponding design based on web survey design principles" [Pop+21b];
- **"Objective 6.7"**: "Define the criteria for selecting an online survey tool that is fit for running the IoTSRM2-based survey" [Pop+21b];
- **"Objective 6.8"**: "Develop the survey analysis plan for the IoTSRM2-based survey to focus the analysis of the survey responses on the research questions of the IoTSRM2-based survey study" [Pop+21b];
- **"Objective 6.9"**: "Set up the IoTSRM2-based survey using the selected online survey tool to meet the applicable survey design principles and to include the questionnaire of the IoTSRM2-based survey" [Pop+21b];
- **"Objective 6.10"**: "Identify the target survey respondents that belong to the target groups of survey respondents and create social media posts and private messages that are aimed at increasing the survey response rate, to request participation in the IoTSRM2-based survey" [Pop+21b];
- **"Objective 6.11"**: "Send requests and reminders for survey participation through different distribution channels, including e-mail and social media (i.e., LinkedIn and Twitter)" [Pop+21b];
- **"Objective 6.12"**: "Analyze the collected survey responses based on the survey analysis plan and report the survey results for part I and II of the IoTSRM2-based survey for all surveyed organizations, the surveyed organizations of the top organization type by survey respondents, and the surveyed organizations from the top industry sector of the top organization type by survey respondents" [Pop+21b].

Furthermore, this step provides "the assumptions on which the survey is based" [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], "these assumptions are split in two types: the underlying assumptions of the IoTSRM2 and the survey methodology assumptions" [Pop+21b]. First, the underlying assumptions of the IoTSRM2 are listed below [Pop+21b]:

- "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 [NIS18a]" [Pop+21a];
- "IoT adopters are assumed to outsource IoT software development and not engage in in-house IoT software development activities" [Pop+21a];
- "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" [Pop+21a].

Second, based on the information disseminated by the author through the research paper [Pop+21b], the assumptions on which the proposed survey methodology is based are listed below:

- "The survey respondents are assumed to provide genuine responses about the surveyed organizations" [Pop+21b];
- "The underlying assumptions of the IoTSRM2 are assumed applicable for the surveyed organizations" [Pop+21b].

In addition, based on the information disseminated by the author through the research paper [Pop+21b], "Step I.1" provides "the limitations of the proposed methodology and survey" [Pop+21b]. These limitations are enumerated below:

- "The proposed survey methodology is derived, based on, and limited to the expert judgement, IoT Security Risk Management Strategy Reference Model (IoTSRM2), and the selected survey design best practice" [Pop+21b];
- "The IoTSRM2-based survey is derived, based on, and limited to the proposed three-phased survey methodology" [Pop+21b];
- "The IoTSRM2-based survey is limited to the assumptions of the proposed survey methodology and the underlying assumptions of the IoTSRM2" [Pop+21b];
- "The IoTSRM2-based survey results are limited to the surveyed organizations and to the responses provided by the survey respondents. It is worth noting that any attempt to draw statistical inferences from the survey data about the current state of the IoT security risk management strategies in other organizations than the ones surveyed should be carefully navigated, is subject to survey biases (e.g., non-response bias, self-reporting bias), and it is beyond the scope of this thesis" [Pop+21b].

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

Based on the information disseminated by the author through the research paper [Pop+21b], "Step I.2" involves "the development of the questionnaire for the IoTSRM2-based survey, which relies on the 30 IoTSRM2 controls from the research article on the IoTSRM2 [Pop+21a]" (see Chapter 5.2) [Pop+21b].

Thus, "the questionnaire is divided into two parts" [Pop+21b]. Part I includes "five screening and background questions" and part II includes "30 IoTSRM2-related questions" [Pop+21b]. "Both parts of the questionnaire contain only closed-ended questions" [Pop+21b].

"With respect to part I of the IoTSRM2-based survey", Table 6.1 "lists the screening and background questions of the questionnaire, and, for each question, it provides the associated possible answers and the justification of question inclusion"

[Pop+21b]. These screening and background questions are used "to ensure the participation of the right survey respondents to the IoTSRM2-based survey and to allow categorization of the survey responses based on the anonymous profiles of the surveyed organizations" [Pop+21b]. Hence, "answering to these questions is a prerequisite for survey respondents to progress to the IoTSRM2-related questions of the IoTSRM2-based survey" [Pop+21b].

Table 6.1. The screening and background questions with possible answers [Pop+21b]

Question ID	Question	Possible Answers	Justification of Question Inclusion
"Q1"	"To which organization are you referring when doing this survey?"	"My organization"	"The sole purpose of this background question is to enhance the collection of survey responses by targeting two types of survey respondents, namely either those from organizations that adopt IoT technologies or those from organizations that help their client organizations embrace IoT technologies" [Pop+21b].
		"My client organization"	
"Q2"	"Which of the following best describes your position?"	"C-level executive and/or board member"	"This screening question aims to ensure the survey participation only of the organizational leaders that belong to the four target groups of survey respondents provided as possible answers for this question" [Pop+21b]. It is worth noting that "Other senior position" refers to "any other senior position of decision-making individuals" [Pop+21b].
		"Consulting practice leader and/or principal"	
		"High-ranking government official"	
		"Other senior position"	
"Q3"	"What is the category of the organization?"	"Large Organization"	"For the purposes of this survey study, the organization type or the organization category is based on the size of the organization, and it can be either small-medium organization or large organization. Hence, this background question aims to allow a clear delineation between the survey responses related to large organizations and those related to small-medium organizations. It is worth noting that SME denotes an organization having, inter
		"Small and Medium Sized Enterprise (SME)"	

Question ID	Question	Possible Answers	Justification of Question Inclusion
			alia, a staff headcount of less than 250 [Eur, n.d]" [Pop+21b].
"Q4"	"In which industry sector does the organization operate?"	"Education"	"This background question aims to allow a clear delineation between the survey responses related to the organizations that operate in different industry sectors" [Pop+21b].
		"Energy & Utilities"	
		"Financial & Insurance Services"	
		"Government"	
		"Healthcare"	
		"Professional Services"	
		"Technology, Media, & Telecom"	
		"Other"	
"Q5"	"In what region is the organization headquartered?"	"Asia"	"This background question aims to allow a clear delineation between the survey responses related to the organizations that are headquartered in different regions" [Pop+21b].
		"Europe, Middle East and Africa (EMEA)"	
		"North/South America"	
		"Oceania"	

Then, "with respect to part II of the IoTSRM2-based survey", Table 6.2 "lists the 30 IoTSRM2-related questions of the IoTSRM2-based survey, and, for each IoTSRM2-related question, it provides the unique identifier of that question and the unique identifier of the corresponding IoTSRM2 control" [Pop+21b]. "Each of these IoTSRM2-related questions is formulated to cover one of the 30 IoTSRM2 controls" presented in Chapter 5.2 and proposed in the research article on the IoTSRM2 [Pop+21a]. Hence, "these IoTSRM2-related questions are designed to get the leaders' views on the current state of the IoT security risk management control strategies of their organizations or client organizations against the IoTSRM2 controls" [Pop+21b].

Table 6.2. The IoTSRM2-related questions [Pop+21b]

Question ID	Question	IoTSRM2 Control ID
"Q6"	"Does the organization have a comprehensive situational awareness on all its IoT hardware assets that leverages cybersecurity bills of materials (CBOMs) for all acquired IoT products and integration with its IT asset management processes?" [Pop+21b]	"AM.A.1"

Question ID	Question	IoTSRM2 Control ID
"Q7"	"Does the organization have a comprehensive situational awareness on all its IoT software assets that leverages cybersecurity bills of materials (CBOMs) for all acquired IoT products and integration with its IT asset management processes?" [Pop+21b]	"AM.B.1"
"Q8"	"Does the organization prioritize all its IoT enabled services (e.g., customer services) and enablers (e.g., IoT components, IoT supply chain) based on their criticality to the organization, using cybersecurity bills of materials (CBOMs) for all acquired IoT products, and leveraging integration with cybersecurity risk management program?" [Pop+21b]	"BE.A.1"
"Q9"	"Does the organization keep, as part of its cybersecurity-related plans, up-to-date documented resiliency requirements (i.e., cybersecurity, reliability, continuity, and recovery) for all its mission critical IoT enabled services, and have high confidence in the cyber resilience of its IoT suppliers?" [Pop+21b]	"BE.B.1"
"Q10"	"Does the organization keep an up-to-date documented IoT security policy that is aligned with wider cybersecurity policy and formally approved, and contract only IoT suppliers that document and maintain robust cybersecurity policies incorporating IoT security considerations?" [Pop+21b]	"GV.A.1"
"Q11"	"Does the organization keep up-to-date documented IoT privacy requirements as part of its privacy policy that is aligned with wider data protection policy and formally approved, and receive privacy supplements from its IoT suppliers for all acquired IoT products and/or services?" [Pop+21b]	"GV.A.2"
"Q12"	"Do the organization's IoT suppliers keep up-to-date vulnerability disclosure policies that are clearly documented, publicly available, aligned with their vulnerability disclosure programs, and well communicated to all stakeholders?" [Pop+21b]	"GV.A.3"
"Q13"	"Do the organization's IoT suppliers keep up-to-date End-of-Life policies that are clearly documented, publicly available, aligned with their product and/or service lifecycle management strategies, and well communicated to all stakeholders?" [Pop+21b]	"GV.A.4"
"Q14"	"Does the organization keep up-to-date documented IoT security governance structures and responsibilities across and within the three lines of defense as part of its cybersecurity risk management program, and define shared governance structures and responsibilities for cybersecurity risk management with its IoT suppliers?" [Pop+21b]	"GV.B.1"
"Q15"	"Does the organization keep up-to-date documented IoT security operations roles and responsibilities as part of its cybersecurity risk management program, have dialogues on shared responsibility for IoT security with its IoT supplies, and maintain up-to-date points of contact for IoT security incident response and vulnerability disclosure from its IoT suppliers?" [Pop+21b]	"GV.B.2"

Question ID	Question	IoTSRM2 Control ID
"Q16"	"Does the organization keep up-to-date documented IoT security and privacy requirements as part of its cybersecurity regulatory framework that is aligned with wider legal and regulatory framework, and work only with IoT suppliers that are aware of IoT security regulatory requirements and are transparent about their compliance with applicable legal and regulatory obligations?" [Pop+21b]	"GV.C.1"
"Q17"	"Does the organization keep an up-to-date documented IoT security and privacy controls management plan that is aligned with its cybersecurity risk management program and approved by board committees and/or C-suite executives, and contract only IoT suppliers that maintain robust cybersecurity-related controls frameworks incorporating IoT security requirements?" [Pop+21b]	"GV.D.1"
"Q18"	"Does the organization keep an up-to-date documented IoT security budget plan that is aligned with its cybersecurity budget plan and approved by board committees and/or C-suite executives, and contract only IoT suppliers that maintain up-to-date cybersecurity budget plans for secure IoT system development lifecycle?" [Pop+21b]	"GV.D.2"
"Q19"	"Does the organization keep an up-to-date documented IoT security measurement and reporting plan that is aligned with its cybersecurity program measurement and reporting and formally approved, and have only IoT suppliers that maintain up-to-date IoT security measurement and reporting plans?" [Pop+21b]	"GV.D.3"
"Q20"	"Does the organization keep an up-to-date documented IoT security training and awareness plan that is aligned with its cybersecurity training and awareness program and formally approved, and have only IoT suppliers that maintain up-to-date IoT security training plans and share up-to-date user guides or manuals for all IoT products and/or services they provide?" [Pop+21b]	"GV.D.4"
"Q21"	"Does the organization keep an up-to-date documented IoT security incident response plan that is aligned with its cybersecurity incident response plan and formally approved, keep dialogues on shared responsibility for incident response with its IoT suppliers, and contract only IoT suppliers that maintain up-to-date cybersecurity incident response plans which incorporate IoT security considerations?" [Pop+21b]	"GV.D.5"
"Q22"	"Does the organization keep an up-to-date documented IoT vulnerability management plan that is aligned with its vulnerability management program and formally approved, and have only IoT suppliers that maintain robust vulnerability management and disclosure plans?" [Pop+21b]	"GV.D.6"
"Q23"	"Does the organization keep an up-to-date documented IoT End-of-Life plan that is aligned with its decommissioning strategy and formally approved, and contract only IoT suppliers that maintain robust End-of-Life policies and are transparent about their sunsetting plans?" [Pop+21b]	"GV.D.7"

Question ID	Question	IoTSRM2 Control ID
"Q24"	"Does the organization continuously identify and document IoT vulnerabilities from multiple external sources as part of its cybersecurity risk assessment process, and have only IoT suppliers that incentivize third-party vulnerability reporting and release timely security advisories for the IoT products and/or services they provide?" [Pop+21b]	"RA.A.1"
"Q25"	"Does the organization continuously or periodically identify and document IoT vulnerabilities using a blend of various assessment processes as part of its cybersecurity risk assessment process, and work only with IoT suppliers that engage in continuous or periodic cybersecurity assessments to achieve ongoing vulnerability monitoring and cybersecurity improvement?" [Pop+21b]	"RA.A.2"
"Q26"	"Does the organization continuously identify and document IoT threats from multiple external threat sharing sources as part of its cybersecurity risk assessment process, and work only with IoT suppliers that engage in cyber threat information sharing and leverage effective vulnerability disclosure programs to identify cyber threats to the IoT products and/or services they provide?" [Pop+21b]	"RA.B.1"
"Q27"	"Does the organization continuously or periodically identify and document IoT threats using a blend of conventional and cyber kill chain based assessments as part of its cybersecurity risk assessment process, and work only with IoT suppliers that engage in cybersecurity assessments to maintain a robust situational awareness on the cyber threats relevant for the IoT products and/or services they provide?" [Pop+21b]	"RA.B.2"
"Q28"	"Does the organization regularly identify and analyze IoT security and privacy risks as part of its cybersecurity risk assessment process, and work only with IoT suppliers that continuously monitor and assess the risks of confidentiality, integrity, availability, and safety of the IoT products and/or services they provide being compromised?" [Pop+21b]	"RA.C.1"
"Q29"	"Does the organization have a comprehensive situational awareness on its IoT security and privacy risks that leverages an up-to-date documented cybersecurity risk register which is aligned with the enterprise cybersecurity risk register, and have high confidence in the cybersecurity risk management capabilities of its IoT suppliers?" [Pop+21b]	"RA.D.1"
"Q30"	"Does the organization clearly articulate and document IoT security risk appetite and tolerances in line with its appetites and tolerances for cybersecurity and privacy risks, and contract only IoT suppliers that are transparent about their appetites and associated tolerances for cybersecurity, privacy, and IoT security risks?" [Pop+21b]	"RM.A.1"
"Q31"	"Does the organization have a comprehensive situational awareness around its role in critical infrastructure and sector risk profile that informs its IoT security risk tolerance statement, and	"RM.B.1"

Question ID	Question	IoTSRM2 Control ID
	have high confidence that the IoT risk tolerances of its IoT suppliers are context-informed?" [Pop+21b]	
"Q32"	"Does the organization keep an up-to-date documented IoT supply chain risk management plan that is aligned with its broader cyber supply chain risk management program and formally approved, and contract only IoT suppliers that maintain robust cyber supply chain risk management plans covering their whole IoT supply chains?" [Pop+21b]	"SC.A.1"
"Q33"	"Does the organization regularly assess and record IoT supply chain risks across its supply chain tiers based on its IoT supply chain risk management plan, and work only with IoT suppliers that continuously or regularly assess their cybersecurity and privacy supply chain risks and are transparent about their findings?" [Pop+21b]	"SC.A.2"
"Q34"	"Does the organization keep an up-to-date documented IoT supplier contract management plan that is aligned with its broader cyber supply chain risk management program and formally approved, and work only with IoT suppliers that maintain robust supplier contract management plans and are transparent about relevant supply chain changes?" [Pop+21b]	"SC.B.1"
"Q35"	"Does the organization keep, as part of its IoT supplier contract management plan, up-to-date documented IoT trustworthiness requirements (i.e., cybersecurity, privacy, safety, reliability, and resiliency) for its IoT supplier contracts, and contract only IoT suppliers that deliver up-to-date cybersecurity bills of materials (CBOMs) for the IoT products they provide and have IoT supplier contracts that enable IoT supply chain of trust?" [Pop+21b]	"SC.B.2"

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], Table 6.3 "outlines the selected answer format for the 30 IoTSRM2-related questions" [Pop+21b]. This table "lists four possible answers, and it gives, for each possible answer, the description of each answer choice and the corresponding percentage score that provides a means to quantitatively rate that answer choice for quantitative analysis of survey responses" [Pop+21b]. Hence, "the answer format of the IoTSRM2-related questions is a four-point Likert scale" with the answer choices "No, to a great extent", "No, to a certain extent", "Yes, to a certain extent", and "Yes, to a great extent", where "the middle point is deliberately excluded to avoid indecisive answers [Rey+19]" [Pop+21b]. Moreover, "these possible answers are designed for survey respondents to rate the extent to which their organizations or client organizations meet each of the IoTSRM2-related questions by selecting one of these answer choices for each of these questions" [Pop+21b].

Table 6.3. The answer format of the IoTSRM2-related questions [Pop+21b]

Possible Answer	Description	Percentage Score
"No, to a great extent"	"The organization's current control deviates from the expected IoTSRM2 control with major discrepancies" [Pop+21b].	"0%"
"No, to a certain extent"	"The organization's current control nearly deviates from the expected IoTSRM2 control with some similarities. This current control state varies across surveyed organizations having a tendency towards deviating from the as-is IoTSRM2 control, which may average around 25% and considers an additional tolerance of 5% to avoid downgrading too much the associated percentage score" [Pop+21b].	"30%"
"Yes, to a certain extent"	"The organization's current control fairly meets the expected IoTSRM2 control with minor discrepancies. This current control state varies across surveyed organizations having a tendency towards meeting the as-is IoTSRM2 control, which may average around 75% and considers a negative tolerance of 5% to avoid favoring too much the associated percentage score" [Pop+21b].	"70%"
"Yes, to a great extent"	"The organization's current control fully meets the expected IoTSRM2 control with no apparent discrepancies" [Pop+21b].	"100%"

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

"Step I.3" involves "the design of the survey based on the principles for designing web questionnaires developed by Dillman et al. (1999) [Dil+99], and on the structure and content of the questionnaire (see Step I.2)" [Pop+21b]. Thus, based on the information disseminated by the author through the research paper [Pop+21b], Table 6.4 "lists these principles for designing web questionnaires, and, for each of these principles, it indicates whether it is applicable to the IoTSRM2-based survey, and it provides the justification of the applicability of that principle" [Pop+21b].

Table 6.4. The applicability of the principles for designing web questionnaires to the IoTSRM2-based survey [Pop+21b]

No.	Principle	Applicability	Justification of Applicability
1.	"Introduce the web questionnaire with a welcome screen that is motivational, emphasizes the ease of responding, and instructs respondents on the action needed for proceeding to the next page." [Dil+99]	"Applicable"	"The IoTSRM2-based survey is designed to have a welcome screen. This welcome screen shows the name of the survey, a thank you message to all the survey participants for taking the time to participate in the survey, the purpose of the survey, the assumptions on which the IoTSRM2 is based, along with the structure of the

No.	Principle	Applicability	Justification of Applicability
			survey. A screenshot of the welcome screen of the IoTSRM2-based survey is provided in Appendix A2 as part of Fig. A2.1" [Pop+21b].
2.	"Begin the web questionnaire with a question that is fully visible on the first screen of the questionnaire, and will be easily comprehended and answered by all respondents." [Dil+99]	"Applicable"	"Following the welcome screen, the IoTSRM2-based survey is designed to begin with a single question that asks the survey respondents to select the organization to which they are referring to when undertaking the survey. A screenshot with the first question from the IoTSRM2-based survey is provided in Appendix A2 as part of Fig. A2.2" [Pop+21b].
3.	"Present each question in a conventional format similar to that normally used on paper questionnaires." [Dil+99]	"Applicable"	"The IoTSRM2-based survey is designed to have each question associated with a unique identifier and to have all possible answers for any given question listed vertically underneath that question" [Pop+21b].
4.	"Limit line length to decrease the likelihood of a long line of prose being allowed to extend across the screen of the respondent's browser." [Dil+99]	"Applicable"	"The IoTSRM2-based survey is structured in two parts: the screening and background questions and the IoTSRM2-related questions (see Step I.2). While the screening and background questions are short, the IoTSRM2-related questions are formulated to cover the entire content of the IoTSRM2 controls, which may increase their length. Notwithstanding, the IoTSRM2-based survey aims to leverage a survey platform that allows this principle being met" [Pop+21b].
5.	"Provide specific instructions on how to take each necessary computer action for responding to the questionnaire." [Dil+99]	"Applicable"	"The welcome screen of the IoTSRM2-based survey is designed to provide sufficient details around the assumptions on which the IoTSRM2 is based and around the structure of the survey. This allows the survey respondents to have visibility on the underlying assumptions of the IoTSRM2 and over the two categories of questions being asked throughout the survey (i.e., the screening and background questions and the IoTSRM2-related questions). In addition, following the first question of the screening and background part, the IoTSRM2-based survey is designed to include a note at the beginning of each page of the questionnaire which is aimed to remind the survey respondents throughout the

No.	Principle	Applicability	Justification of Applicability
			questionnaire what the word Organization denotes (i.e., their organization or client organization depending on their answer to the first question of the IoTSRM2-based survey)" [Pop+21b].
6.	"Provide computer operation instructions as part of each question where the action is to be taken, not in a separate section prior to the beginning of the questionnaire." [Dil+99]	"Applicable"	"The IoTSRM2-based survey is designed to notify the survey respondents through an error message about any unanswered questions from any given page before being allowed to move to the next page. In addition, the questionnaire targets only computer literate respondents and is designed to include only closed-ended questions. Thus, there is no other need for computer operation instructions or specific response instructions" [Pop+21b].
7.	"Do not require respondents to provide an answer to each question before being allowed to answer any subsequent ones." [Dil+99]	"Applicable"	"The IoTSRM2-based survey is designed to allow the survey respondents to respond to questions in any order within any page of the survey" [Pop+21b].
8.	"Construct web questionnaires so that they scroll from question to question unless order effects are a major concern, large numbers of questions must be skipped, and/or a mixed-mode survey is being done for which telephone interview and web results will be combined." [Dil+99]	"Applicable"	"The multipage IoTSRM2-based survey is designed to allow the survey respondents to scroll from question to question within any page of the survey, and the navigation from one page to another is conditioned by the completion of all actions from that page. Also, following the first question of the screening and background part, the IoTSRM2-based survey is designed to include a note at the beginning of each page of the questionnaire which reminds the survey respondents what the word Organization denotes (i.e., their organization or client organization) and encourages them to review their response to question 1 if necessary" [Pop+21b].
9.	"When the number of answer choices exceeds the number that can be displayed on one screen, consider double-banking with appropriate navigational instructions being added." [Dil+99]	"Not applicable"	"The IoTSRM2-based survey is designed to display all answer choices on the screen in a visible manner for all questions" [Pop+21b].

No.	Principle	Applicability	Justification of Applicability
10.	"Use graphical symbols or words that convey a sense of where the respondent is in the completion progress, but avoid ones that require advanced programming." [Dil+99]	"Applicable"	"The IoTSRM2-based survey is designed to have a progress bar that allow respondents to have visibility on their completion progress. The progress bar can be observed in the screenshot provided in Appendix A2 as part of Fig. A2.1" [Pop+21b].
11.	"Be cautious about using question structures that have known measurement problems on paper questionnaires, e.g., check-all-that-apply and open-ended questions." [Dil+99]	"Applicable"	"The IoTSRM2-based survey is designed to include only closed-ended questions that are measurable (see Step I.2)" [Pop+21b].

Furthermore, "Step I.3" provides "the criteria defined for the selection of the online survey tool which is used to set up and run the IoTSRM2-based survey" [Pop+21b]. Thus, based on the information disseminated by the author through the research paper [Pop+21b], Table 6.5 "provides these selection criteria, and it outlines, for each selection criterion, the corresponding justification of inclusion for the selection of the online survey tool" [Pop+21b].

Table 6.5. The criteria for selecting the online survey tool [Pop+21b]

No.	Selection Criterion	Justification of Inclusion
1.	"The online survey tool provides features that allow the creation of the online IoTSRM2-based survey following the principles for designing web questionnaires developed by Dillman et al. [Dil+99]." [Pop+21b]	"The online survey tool of choice should allow the creation of the online IoTSRM2-based survey based on the web survey design principles developed by Dillman et al. (1999) [Dil+99], which will make way for a better survey experience for the respondents and a higher response rate." [Pop+21b]
2.	"The online survey tool allows for anonymous responses." [Pop+21b]	"The online survey tool should keep the data of the respondents anonymous to encourage the survey respondents to share their views without being worried of breaching confidentiality and non-disclosure agreements. This may boost the response rate and improve the quality of survey responses." [Pop+21b]
3.	"The online survey tool allows the inclusion of the 35 questions of the questionnaire." [Pop+21b]	"The online survey tool should accommodate the inclusion of the 35-items questionnaire to allow the collection of survey responses to the screening and background questions and to the 30 IoTSRM2-related questions." [Pop+21b]
4.	"The online survey tool provides the feature that allows the creation of mobile friendly surveys." [Pop+21b]	"The online survey tool should have the mobile friendly feature giving that the IoTSRM2-based survey is targeting leaders

No.	Selection Criterion	Justification of Inclusion
		and seniors who are frequently using mobile devices, and the intent is that the IoTSRM2-based survey to be available for both desktop and mobile devices." [Pop+21b]
5.	"The online survey tool provides the feature that allows the export of the survey responses in the Excel file format." [Pop+21b]	"The online survey tool should provide the ability of exporting the survey responses in the Excel file format. This is because the analysis of the survey responses will use the Excel software." [Pop+21b]
6.	"The online survey tool is a well renowned online survey tool." [Pop+21b]	"Running the IoTSRM2-based survey using a widely used online survey tool may increase the likelihood that the target survey respondents respond to the survey." [Pop+21b]

Thus, "considering the six selection criteria outlined above, the SurveyMonkey tool is selected for the creation of the IoTSRM2-based survey" [Pop+21b]. Moreover, "the setup of the IoTSRM2-based survey is guided by the principles for designing web questionnaires developed by Dillman et al. (1999) [Dil+99], uses the Momentive's guidance for creating a survey [Mom21], follows the structure of the questionnaire (see Step I.2), and includes the content of the questionnaire (see Step I.2)" [Pop+21b]. In addition, "this setup activity involves the testing of the IoTSRM2-based survey prior to having it up and running" [Pop+21b].

Furthermore, "Step I.3" involves "the development of the survey analysis plan to ensure that the outputs of the proposed methodology help in addressing the research questions" [Pop+21b]. Irwin and Stafford (2016) [Irw+16] "endorsed this approach to ensure that the development of the survey is on track with the intended survey outcomes" [Pop+21b].

Thus, based on the information disseminated by the author through the research paper [Pop+21b], Table 6.6 "outlines the survey analysis plan which maps the survey questions (i.e., IoTSRM2-Based Survey Question ID), the intended analysis method (i.e., Potential Analysis Method), and the intended presentation of the results (i.e., Potential Presentation of Results) to each of the research questions and its corresponding unique identifier" [Pop+21b].

Table 6.6. The proposed survey analysis plan [Pop+21b]

Research Question ID	Research Question	IoTSRM2 Based Survey Question IDs	Potential Analysis Method	Potential Presentation Of Results
"RQ1"	"What is the overall tendency of the IoT security risk management strategies of the surveyed organizations to meet or deviate	"Q6-Q35"	"For each IoTSRM2 control and related question: % of survey responses of" ("Yes, to a certain extent" and "Yes, to a great extent") "compared with % of survey	"Figure showing, for each IoTSRM2 control and related question, the overall tendency of the survey responses towards either deviating from or meeting that

Research Question ID	Research Question	IoTSRM2 Based Survey Question IDs	Potential Analysis Method	Potential Presentation Of Results
	from the IoTSRM2 controls?" [Pop+21b]		responses of" ("No, to a great extent" and "No, to a certain extent") [Pop+21b]	IoTSRM2 control" [Pop+21b].
"RQ2"	"What is the IoTSRM2 compliance score of each of the surveyed organizations?" [Pop+21b]	"Q6-Q35"	"For each surveyed organization: IoTSRM2 compliance score" [Pop+21b]	"Column chart showing, for each surveyed organization, the IoTSRM2 compliance score, corresponding region, and whether this score is less than 50% or greater or equal to 50%" [Pop+21b].
"RQ3"	"Which is the top organization type for the surveyed organizations by survey respondents?" [Pop+21b]	"Q3"	"% distribution of the survey responses by organization type" [Pop+21b]	"Pie chart showing the % distribution of the responses to the IoTSRM2-based survey by organization type for the surveyed organizations" [Pop+21b].
"RQ4.a"	"Which is the top industry sector for the surveyed organizations by survey respondents?" [Pop+21b]	"Q4"	"% distribution of the survey responses by industry sector for the surveyed organizations" [Pop+21b]	"Pie chart showing the % distribution of the responses by industry sector for the surveyed organizations" [Pop+21b].
"RQ4.b"	"Which is the top industry sector for the surveyed organizations of the top organization type by survey respondents?" [Pop+21b]	"Q3-Q4"	"% distribution of the survey responses by industry sector for the surveyed organizations of the top organization type" [Pop+21b]	"Pie chart showing the % distribution of the responses by industry sector for the surveyed organizations of the top organization type" [Pop+21b].
"RQ5.a"	"What is the overall average IoTSRM2 compliance score of the surveyed organizations for each IoTSRM2 control?" [Pop+21b]	"Q6-Q35"	"For each IoTSRM2 control and related question: Overall average compliance score of surveyed organizations with IoTSRM2 controls" [Pop+21b]	"Figure showing, for each IoTSRM2 control and related question, the overall average IoTSRM2 compliance score of the surveyed organizations and whether this score is

Research Question ID	Research Question	IoTSRM2 Based Survey Question IDs	Potential Analysis Method	Potential Presentation Of Results
				less than 50% or greater or equal to 50%" [Pop+21b].
"RQ5.b"	"What is the overall average IoTSRM2 compliance score of the surveyed organizations of the top organization type for each IoTSRM2 control?" [Pop+21b]	"Q6-Q35"	"For each IoTSRM2 control and related question: Overall average compliance score of surveyed organizations of the top organization type with IoTSRM2 controls" [Pop+21b]	"Figure showing, for each IoTSRM2 control and related question, the overall average IoTSRM2 compliance score of the surveyed organizations of the top organization type and whether this score is less than 50% or greater or equal to 50%" [Pop+21b].
"RQ5.c"	"What is the overall average IoTSRM2 compliance score of the surveyed organizations from the top industry sector of the top organization type for each IoTSRM2 control?" [Pop+21b]	"Q6-Q35"	"For each IoTSRM2 control and related question: Overall average compliance score of surveyed organizations from the top industry sector of the top organization type with IoTSRM2 controls" [Pop+21b]	"Figure showing, for each IoTSRM2 control and related question, the overall average IoTSRM2 compliance score of the surveyed organizations from the top industry sector of the top organization type and whether this score is less than 50% or greater or equal to 50%" [Pop+21b].
"RQ6.a"	"Which is the top position level of the survey respondents for the surveyed organizations by survey respondents?" [Pop+21b]	"Q2"	"% distribution of the survey respondents by position level for the surveyed organizations" [Pop+21b]	"Pie chart showing the % distribution of the survey respondents by position level for the surveyed organizations" [Pop+21b].
"RQ6.b"	"Which is the top position level of the survey respondents for the surveyed organizations of the top organization type by survey respondents?" [Pop+21b]	"Q2-Q3"	"% distribution of the survey respondents by position level for the surveyed organizations of the top organization type" [Pop+21b]	"Pie chart showing the % distribution of the survey respondents by position level for the surveyed organizations of the top organization type" [Pop+21b].
"RQ6.c"	"Which is the top position level of the	"Q2-Q4"	"% distribution of the survey respondents by	"Pie chart showing the % distribution of the

Research Question ID	Research Question	IoTSRM2 Based Survey Question IDs	Potential Analysis Method	Potential Presentation Of Results
	survey respondents for the surveyed organizations from the top industry sector of the top organization type by survey respondents?” [Pop+21b]		position level for the surveyed organizations from the top industry sector of the top organization type” [Pop+21b]	survey respondents by position level for the surveyed organizations from the top industry sector of the top organization type” [Pop+21b].
“RQ7.a”	“Which is the top region for the surveyed organizations by survey respondents?” [Pop+21b]	“Q5”	“% distribution of the survey responses by region for the surveyed organizations” [Pop+21b]	“Pie chart showing the % distribution of the survey responses by region for the surveyed organizations” [Pop+21b].
“RQ7.b”	“Which is the top region for the surveyed organizations of the top organization type by survey respondents?” [Pop+21b]	“Q3, Q5”	“% distribution of the survey responses by region for the surveyed organizations of the top organization type” [Pop+21b]	“Pie chart showing the % distribution of the survey responses by region for the surveyed organizations of the top organization type” [Pop+21b].
“RQ7.c”	“Which is the top region for the surveyed organizations from the top industry sector of the top organization type by survey respondents?” [Pop+21b]	“Q3-Q5”	“% distribution of the survey responses by region for the surveyed organizations from the top industry sector of the top organization type” [Pop+21b]	“Pie chart showing the % distribution of the survey responses by region for the surveyed organizations from the top industry sector of the top organization type” [Pop+21b].

6.2.2. Phase II: Launch and Run

Based on the information disseminated by the author through the research paper [Pop+21b], the “Launch and Run” phase involves “the request for participation in the IoTSRM2-based survey (Step II.1), the submission of reminders about the IoTSRM2-based survey (Step II.2), and the export of survey responses to Excel and the rejection of incomplete survey responses (Step II.3)” [Pop+21b].

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

Based on the information disseminated by the author through the research paper [Pop+21b], “Step II.1” involves “the identification of target survey respondents for the sampling frame, and the request for participation of the target respondents in the IoTSRM2-based survey” [Pop+21b]. First, the identification of the target survey respondents is based on “the target groups of survey respondents selected in Step I.2” [Pop+21b]. Second, the request for participation in the IoTSRM2-based survey entails “the creation of social media posts and private messages for requesting participation in the IoTSRM2-based survey, and the delivery of these messages using the distribution channels decided on in Step I.1” [Pop+21b].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], “the social media posts and private messages for requesting participation in the survey, are designed to increase the response rate of the survey by employing several widely used techniques” [Pop+21b]. First, “the private messages leverage personalization for engaging with each of the target survey respondents as described by Frippiat and Marquis (2010) [Fri+10]” [Pop+21b]. Moreover, “the social media posts and private messages apply three of the survey responses theories (i.e., exchange theory, self-perception theory, and commitment and involvement) studied by Keusch (2015) [Keu15]” [Pop+21b]. These theories “were also employed in the study conducted by Poon et al. (2004) [Poo+04] to invite or induce participation as part of a laboratory-type experiment” [Pop+21b]. Thus, based on the information disseminated by the author through the research paper [Pop+21b], “besides providing key details on the IoTSRM2-based survey (e.g., the access link to the survey), the social media posts and private messages feature a combination of the following techniques” [Pop+21b]:

- **“Personalization”:** “the private messages are personalized for engaging with each of the target survey respondents by starting the message with an informal greeting (e.g., Hello John)” [Pop+21b];
- **“Exchange theory”:** “the private messages ask the target survey respondents to complete the survey and/or share it to the right individuals from their teams for getting access to the survey results once these get published (i.e., Once our next article is published, you will be able to benchmark your organization or client organization against peers)” [Pop+21b];
- **“Self-perception theory”:** “the self-perception theory is applied as part of the social media posts by asking prestigious IoT-engaged leaders to complete the survey and/or share it to the right individuals from their teams, which labels them as being IoT engaged (i.e., we are please asking prestigious IoT-engaged leaders to share their views and or share our survey with the right people)” [Pop+21b];
- **“Commitment/involvement”:** “the social media posts and private messages clearly articulate the importance of the IoTSRM2-based survey topic (e.g., IoTSRM2 relies on 25 IoT security best practices and is the result of an extensive research work) and of participating in the IoTSRM2-based survey by getting the chance to have their opinions heard (i.e., Our survey seeks views from leaders from industries and governments on the IoT security risk management strategies of their organizations or client organizations)” [Pop+21b].

“Step II.2”: “Send reminders about the IoTSRM2-based survey”

Based on the information disseminated by the author through the research paper [Pop+21b], “Step II.2” involves “sending a combination of reminders including private messages and social media posts about the IoTSRM2-based survey” [Pop+21b]. This activity of using a blend of reminders aims “to reduce the number of individual reminders being sent and to increase the survey response rate” [Pop+21b]. According to the studies conducted by Keusch (2015) [Keu15] and Sánchez-Fernández et al. (2012) [Sán+12], “sending a reduced number of reminders is considered to have a positive influence on survey response rates” [Pop+21b].

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

Based on the information disseminated by the author through the research paper [Pop+21b], "Step II.3" involves "the export of all survey responses from SurveyMonkey to Excel once the survey ends" [Pop+21b]. At this point, "all individual survey responses that are incomplete are discarded to ensure only clean survey responses are retained for the analysis and reporting" [Pop+21b].

6.2.3. Phase III: Analyze and Report

Based on the information disseminated by the author through the research paper [Pop+21b], the "Analyze and Report" phase involves "obtaining quantitative figures for the survey responses on top of the original survey responses (Step III.1), the qualitative and quantitative analysis of the IoTSRM2-based survey responses (Step III.2), and the reporting of the IoTSRM2-based survey results (Step III.3)" [Pop+21b].

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

Based on the information disseminated by the author through the research paper [Pop+21b], "Step III.1" involves "retaining the exported survey responses in their original form and converting a copy of the qualitative IoTSRM2-related responses into quantitative figures as outlined in the study conducted by Combs and Onwuegbuzie (2010) [Com+10]" [Pop+21b]. "This translation of survey responses into quantitative figures leverages the percentage scores corresponding to the possible answers of the IoTSRM2-related questions (see Step I.2)" [Pop+21b].

Hence, "for each survey respondent, the quantitative figures (i.e., the percentage scores) are represented using Equation (6.1)", where "Q_j represents the 30 IoTSRM2-related questions (i.e., from Q6 to Q35), $\text{Response}_i(Q_j)$ represents the responses of the survey respondents to the IoTSRM2-related questions, R_{ij} represents the percentage scores corresponding to survey respondents for the IoTSRM2-related questions (see Step I.2), and K represents the cardinality of the survey respondents" [Pop+21b]:

$$\begin{gathered}\text{Convert }(\text{Response}_i(Q_j))=R_{ij},\\ \text{where } R_{ij}=\begin{cases} 0, \text{Response}_i(Q_j)=\text{"No, to a great extent"} \\ 30\%, \text{Response}_i(Q_j)=\text{"No, to a certain extent"} \\ 70\%, \text{Response}_i(Q_j)=\text{"Yes, to a certain extent"} \\ 100\%, \text{Response}_i(Q_j)=\text{"Yes, to a great extent"} \end{cases}\\ i=[1..K],\ j=[6..35],\text{ and } K=|\text{survey respondents}|\end{gathered}\tag{6.1}$$

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

Based on the information disseminated by the author through the research paper [Pop+21b], this step involves "the analysis of all survey responses across three groups of surveyed organizations" [Pop+21b]. First, "the analysis is performed across all surveyed organizations" [Pop+21b]. Second, "the analysis focuses on the surveyed organizations of top organization type by survey respondents" [Pop+21b]. Finally, "the analysis is conducted on the surveyed organizations from the top industry sector of the top organization type by survey respondents" [Pop+21b].

Thus, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.3 shows "the overview of the intended analysis of the survey responses for part I and II of the IoTSRM2-based survey across three groups of surveyed organizations" [Pop+21b].

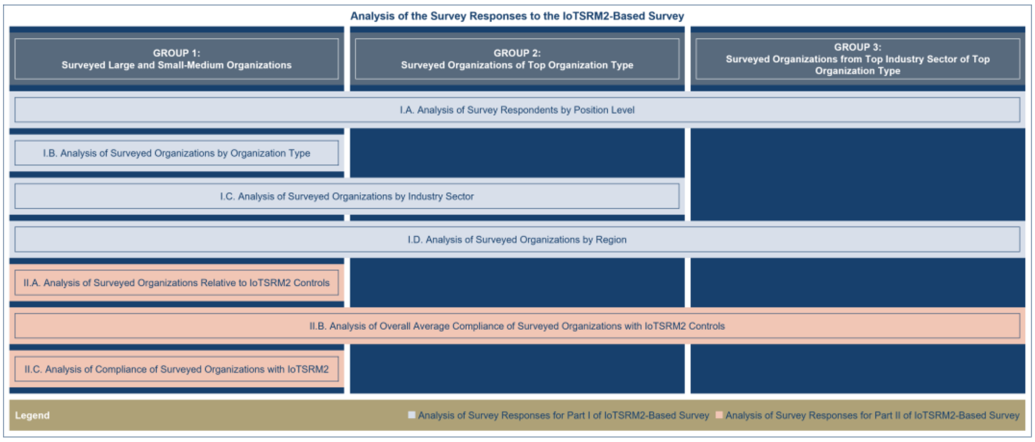

Analysis of the Survey Responses to the IoTSRM2-Based Survey
GROUP 1: Surveyed Large and Small-Medium Organizations
GROUP 2: Surveyed Organizations of Top Organization Type
GROUP 3: Surveyed Organizations from Top Industry Sector of Top Organization Type
I.A. Analysis of Survey Respondents by Position Level
I.B. Analysis of Surveyed Organizations by Organization Type
I.C. Analysis of Surveyed Organizations by Industry Sector
I.D. Analysis of Surveyed Organizations by Region
II.A. Analysis of Surveyed Organizations Relative to IoTSRM2 Controls
II.B. Analysis of Overall Average Compliance of Surveyed Organizations with IoTSRM2 Controls
II.C. Analysis of Compliance of Surveyed Organizations with IoTSRM2
Legend
Analysis of Survey Responses for Part I of IoTSRM2-Based Survey
Analysis of Survey Responses for Part II of IoTSRM2-Based Survey

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

Thus, "with respect to the analysis of the survey responses for part I of the IoTSRM2-based survey", based on the information disseminated by the author through the research paper [Pop+21b], first, "the analysis of survey respondents by position level (i.e., I.A) is intended across all three groups of surveyed organizations (i.e., the surveyed large and small-medium organizations, the surveyed organizations of the top organization type, and the surveyed organizations from the top industry sector of the top organization type)" [Pop+21b]. This analysis (i.e., "I.A") "aims to address the RQ6.a, RQ6.b, and RQ6.c research questions (see Step I.3), and it involves exploring the percentage distribution of the survey respondents by position level for each group of survey respondents" [Pop+21b]. Second, "the analysis of the surveyed organizations by organization type (i.e., I.B) is intended for the first group of surveyed organizations" [Pop+21b]. This analysis (i.e., "I.B") "aims to address the RQ3 research question (see Step I.3), and it involves exploring the percentage distribution of the surveyed organizations by organization type for the surveyed large and small-medium organizations" [Pop+21b]. Third, "the analysis of the surveyed organizations by industry sector (i.e., I.C) is intended for the first two groups of surveyed organizations" [Pop+21b]. This analysis (i.e., "I.C") "aims to address the RQ4.a and RQ4.b research questions (see Step I.3), and it involves exploring the percentage distribution of the surveyed organizations by industry sector for the surveyed large and small-medium organizations and for the surveyed organizations of top organization type" [Pop+21b]. Finally, "the analysis of the surveyed organizations by region (i.e., I.D) is intended to span all three groups of surveyed organizations" [Pop+21b]. This analysis (i.e., "I.D") "aims to address the RQ7.a, RQ7.b, and RQ7.c research questions (see Step I.3), and it involves exploring the percentage distribution of the surveyed organizations by region for all three groups of surveyed organizations" [Pop+21b].

Then, "with respect to the analysis of the survey responses for part II of the IoTSRM2-based survey", based on the information disseminated by the author through the research paper [Pop+21b], first, "the analysis of the surveyed organizations relative to the IoTSRM2 controls (i.e., II.A) is intended for the first group of surveyed organizations" [Pop+21b]. This analysis (i.e., "II.A") "aims to address the RQ1 research question (see Step I.3), and it involves examining the survey responses in their qualitative form" by comparing, for each "IoTSRM2-related question", "the percentage of survey responses" of "Yes, to a certain extent" and "Yes, to a great extent" against "the percentage of survey responses" of "No, to a great extent" and "No, to a certain extent" [Pop+21b].

Second, "the analysis of the overall average compliance of the surveyed organizations with the IoTSRM2 controls (i.e., II.B) is intended for all three groups of surveyed organizations" [Pop+21b]. This analysis (i.e., "II.B") "aims to address the RQ5.a, RQ5.b and RQ5.c research questions (see Step I.3), and it involves computing, for each IoTSRM2 control and related question for each of the three groups of surveyed organizations, the overall average compliance score based on the quantitative figures for the survey responses and the corresponding adjusted control weight" [Pop+21b].

Hence, first, "for each survey respondent and for each IoTSRM2 control and related question", this analysis (i.e., "II.B") "feeds the quantitative figures that result from using Equation (6.1) (see Step III.1) together with the corresponding adjusted control weight (see Chapter 5.2) into Equation (6.2) to determine the compliance of the corresponding surveyed organization with that IoTSRM2 control and related question" [Pop+21b]. Note that "in Equation (6.2), $\text{Compliance}_i(C_j)$ represents the compliance scores of the surveyed organizations with the IoTSRM2 controls, C_j represents the IoTSRM2 controls that correspond to the IoTSRM2-related questions (see Tables 5.4, 5.7, 5.12, 5.17,5.20, and 5.23 from Chapter 5.2 and Table 6.2 from Chapter 6.2.1), R_{ij} represents the percentage scores corresponding to survey respondents for the IoTSRM2-related questions (see Step III.1), Adjusted weight (C_j) represents the adjusted weights corresponding to the IoTSRM2 controls (see Tables 5.4, 5.7, 5.12, 5.17,5.20, and 5.23 from Chapter 5.2), and K represents the cardinality of the survey respondents" [Pop+21b].

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

Second, "after computing the compliance score with each of the IoTSRM2 controls for each of the surveyed organizations", this analysis (i.e., "II.B") "is intended for each of the three groups of surveyed organizations and aims to determine, for each IoTSRM2 control and related question, the overall average compliance score and whether this score shows a tendency towards deviating from (i.e., less than 50%) or meeting (i.e., greater than or equal to 50%) the as-is IoTSRM2 control" [Pop+21b]. These overall average compliance scores "are represented using Equation (6.3), where L_k represents the cardinality of the survey respondents for the Group k of surveyed organizations (i.e., the Group 1, Group 2, and Group 3), $\text{Compliance}_i(C_j)$ represents the compliance scores of the surveyed organizations with the IoTSRM2 controls, and C_j represents the IoTSRM2 controls that correspond to the IoTSRM2-

related questions (see Tables 5.4, 5.7, 5.12, 5.17,5.20, and 5.23 from Chapter 5.2 and Table 6.2 from Chapter 6.2.1)" [Pop+21b].

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

Finally, "the analysis of the compliance of the surveyed organizations with IoTSRM2 (i.e., II.C) is intended for the first group of surveyed organizations" [Pop+21b]. This analysis (i.e., "II.C") "aims to address the RQ2 research question (see Step I.3), and it involves determining, for each of the surveyed organizations, the IoTSRM2 compliance score using Equation (6.4)" [Pop+21b]. In this equation, "$\text{IoTSRM2 compliance score}_i$ represents the IoTSRM2 compliance scores of the surveyed organizations, $\text{Compliance}_i(C_j)$ represents the compliance scores of the surveyed organizations with the IoTSRM2 controls, C_j represents the IoTSRM2 controls that correspond to the IoTSRM2-related questions (see Tables 5.4, 5.7, 5.12, 5.17,5.20, and 5.23 from Chapter 5.2 and Table 6.2 from Chapter 6.2.1), and K represents the cardinality of the survey respondents" [Pop+21b].

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

Moreover, "to allow for the anonymous nature of and enable an easier analysis and understanding of the survey responses", this analysis (i.e., "II.C") "leverages the proposed naming convention for identifying each of the surveyed organizations, where name parts are separated by dots" [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], these name parts are outlined below:

- "The organization category identifier, which shows the type of the organization in question", specifically: "LG" for "Large Organizations" or "SM" for "Small-Medium Organizations" [Pop+21b];
- "The industry classification identifier, which shows the industry sector of the organization in question", specifically: "EDU" for "Education", "E&U" for "Energy & Utilities", "FSO" for "Financial & Insurance Services", "GOV" for "Government", "HSO" for "Healthcare", "PSO" for "Professional Services", "TMT" for "Technology, Media, & Telecom", or "OTH" for "Other" [Pop+21b];
- "The sequence number of the organization within the group of surveyed organizations of the same organization category and industry sector" [Pop+21b].

For instance, "LG.TMT.1 denotes the first surveyed large organization from the Technology, Media, & Telecom (TMT) industry sector, while the SM.TMT.1 denotes the first surveyed small medium organization from the Technology, Media, & Telecom (TMT) industry sector" [Pop+21b].

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

Based on the information disseminated by the author through the research paper [Pop+21b], this step involves "the reporting of the IoTSRM2-based survey results for each of the three groups of surveyed organizations outlined in Step III.2" [Pop+21b], namely:

- **"Group 1":** "the surveyed large and small-medium organizations" [Pop+21b];
- **"Group 2":** "the surveyed organizations of the top organization type" [Pop+21b];
- **"Group 3":** "the surveyed organizations from the top industry sector of the top organization type" [Pop+21b].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.4 "provides the intended structure for reporting the IoTSRM2-based survey findings" [Pop+21b].

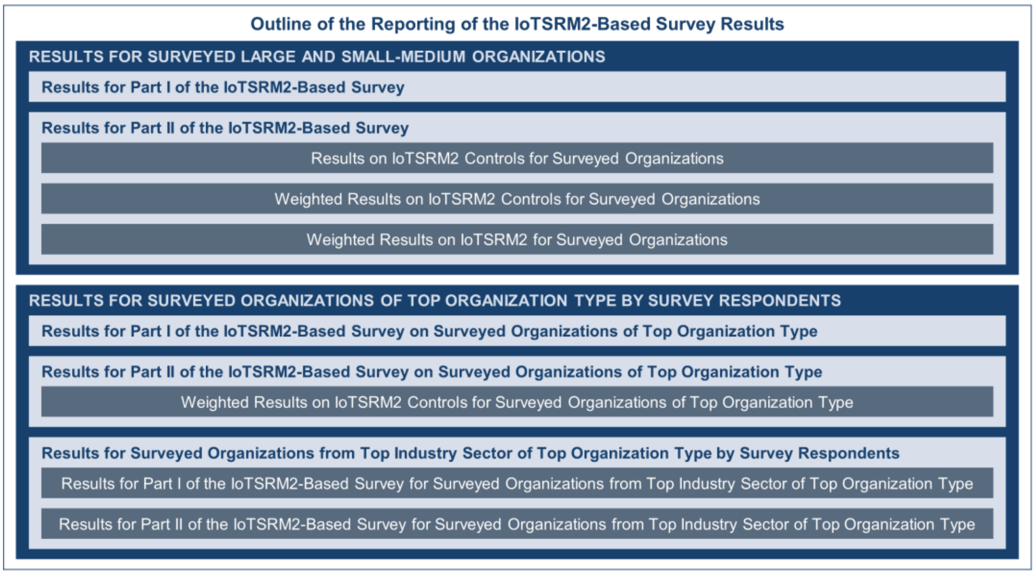

Outline of the Reporting of the IoTSRM2-Based Survey Results
RESULTS FOR SURVEYED LARGE AND SMALL-MEDIUM ORGANIZATIONS
Results for Part I of the IoTSRM2-Based Survey
Results for Part II of the IoTSRM2-Based Survey
Results on IoTSRM2 Controls for Surveyed Organizations
Weighted Results on IoTSRM2 Controls for Surveyed Organizations
Weighted Results on IoTSRM2 for Surveyed Organizations
RESULTS FOR SURVEYED ORGANIZATIONS OF TOP ORGANIZATION TYPE BY SURVEY RESPONDENTS
Results for Part I of the IoTSRM2-Based Survey on Surveyed Organizations of Top Organization Type
Results for Part II of the IoTSRM2-Based Survey on Surveyed Organizations of Top Organization Type
Weighted Results on IoTSRM2 Controls for Surveyed Organizations of Top Organization Type
Results for Surveyed Organizations from Top Industry Sector of Top Organization Type by Survey Respondents
Results for Part I of the IoTSRM2-Based Survey for Surveyed Organizations from Top Industry Sector of Top Organization Type
Results for Part II of the IoTSRM2-Based Survey for Surveyed Organizations from Top Industry Sector of Top Organization Type

Fig. 6.4. Outline of the reporting for the IoTSRM2-based survey results [Pop+21b]

Hence, "with respect to the Group 1 of surveyed organizations", the reporting involves [Pop+21b]:

- "Providing the survey results derived from the analysis (i.e., I.A, I.B, I.C, I.D) of the survey responses for part I of the IoTSRM2-based survey (see Step III.2)" [Pop+21b];
- "Providing the survey results derived from the analysis (i.e., II.A, II.B, II.C) of the survey responses for part II of the IoTSRM2-based survey (see Step III.2)" [Pop+21b].

Then, "with respect to the Group 2 of surveyed organizations", the reporting involves [Pop+21b]:

- "Providing the survey results derived from the analysis (i.e., I.A, I.C, I.D) of the survey responses for part I of the IoTSRM2-based survey (see Step III.2)" [Pop+21b];
- "Providing the survey results derived from the analysis (i.e., II.B) of the survey responses for part II of the IoTSRM2-based survey (see Step III.2)" [Pop+21b].

Finally, "with respect to the Group 3 of surveyed organizations", the reporting involves [Pop+21b]:

- "Providing the survey results derived from the analysis (i.e., I.A, I.D) of the survey responses for part I of the IoTSRM2-based survey (see Step III.2)" [Pop+21b];
- "Providing the survey results derived from the analysis (i.e., II.B) of the survey responses for part II of the IoTSRM2-based survey (see Step III.2)" [Pop+21b].

6.3. The Results of the IoTSRM2-Based Survey

Based on the information disseminated by the author through the research paper [Pop+21b], this subchapter presents the IoTSRM2-based survey results and is structured in two sub-subchapters as depicted in Fig. 6.5 [Pop+21b]. Chapter 6.3.1 "focuses on the survey results for the surveyed large and small-medium organizations" [Pop+21b]. First, Chapter 6.3.1.1 "provides the results for part I of the IoTSRM2-based survey" [Pop+21b]. Second, Chapter 6.3.1.2 "provides the results for part II of the IoTSRM2-based survey by focusing on the IoTSRM2 controls and on the entire IoTSRM2 for the surveyed organizations" [Pop+21b]. Subsequently, Chapter 6.3.2 "focuses exclusively on the survey results for the surveyed organizations of the top organization type by survey respondents (see Chapter 6.2), namely on the surveyed large organizations" [Pop+21b]. First, Chapter 6.3.2.1 "provides the results for part I of the IoTSRM2-based survey on the surveyed large organizations" [Pop+21b]. Second, Chapter 6.3.2.2 "provides the results for part II of the IoTSRM2-based survey on the surveyed large organizations by focusing on the corresponding IoTSRM2 controls" [Pop+21b]. Third, Chapter 6.3.2.3 "narrows the focus on the surveyed large organizations from the top industry sector by survey respondents (see Chapter 6.2), namely on the surveyed large organizations from the Technology, Media, and Telecom (TMT) industry sector, and provides the results for part I and II of the IoTSRM2-based survey on the surveyed large TMT organizations" [Pop+21b].

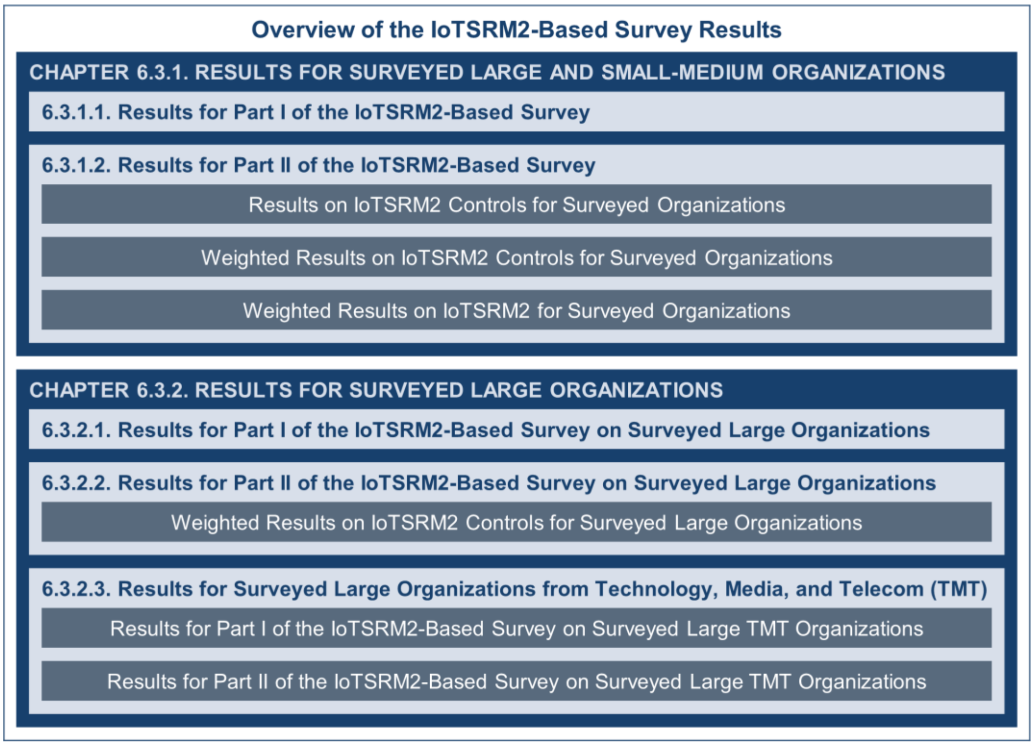

Overview of the IoTSRM2-Based Survey Results
CHAPTER 6.3.1. RESULTS FOR SURVEYED LARGE AND SMALL-MEDIUM ORGANIZATIONS
6.3.1.1. Results for Part I of the IoTSRM2-Based Survey
6.3.1.2. Results for Part II of the IoTSRM2-Based Survey
Results on IoTSRM2 Controls for Surveyed Organizations
Weighted Results on IoTSRM2 Controls for Surveyed Organizations
Weighted Results on IoTSRM2 for Surveyed Organizations
CHAPTER 6.3.2. RESULTS FOR SURVEYED LARGE ORGANIZATIONS
6.3.2.1. Results for Part I of the IoTSRM2-Based Survey on Surveyed Large Organizations
6.3.2.2. Results for Part II of the IoTSRM2-Based Survey on Surveyed Large Organizations
Weighted Results on IoTSRM2 Controls for Surveyed Large Organizations
6.3.2.3. Results for Surveyed Large Organizations from Technology, Media, and Telecom (TMT)
Results for Part I of the IoTSRM2-Based Survey on Surveyed Large TMT Organizations
Results for Part II of the IoTSRM2-Based Survey on Surveyed Large TMT Organizations

Fig. 6.5. Outline of the structure of the IoTSRM2-based survey results [Pop+21b]

6.3.1. Results for Surveyed Large and Small-Medium Organizations

Chapter 6.3.1 is structured in two sub-sub-subchapters [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], first it “provides the results for part I of the IoTSRM2-based survey, and then it provides the results for part II of the IoTSRM2-based survey” [Pop+21b].

Following the IoTSRM2-based survey, which “was conducted between 14 June and 12 July 2021” and based on the information disseminated by the author through the research paper [Pop+21b], Table 6.7 shows “the key details on the responses to the IoTSRM2-based survey including the sampling frame of 1,502 leaders and seniors with stake in cybersecurity and/or technology risk management strategies, the number of collected individual survey responses (i.e., the survey returns), the number of discarded surveys (see Step II.3 of the Launch and Run phase of the survey methodology from Chapter 6.2), the final sample of 31 leaders and seniors with stake in IoT security risk management strategies, and the survey response rate of 2.1%” [Pop+21b].

Table 6.7. Key details on the responses to the IoTSRM2-based survey [Pop+21b]

Sampling Frame	Survey Returns	Discarded Surveys	Final Sample	Survey Response Rate
"1,502" [1]	"63"	"32"	"31"	"2.1%"

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

6.3.1.1 Results for Part I of the IoTSRM2-Based Survey

Based on the information disseminated by the author through the research paper [Pop+21b], Chapter 6.3.1.1 "provides the main results for part I of the IoTSRM2-based survey including the percentage distribution of the survey respondents by position level, and the percentage distributions of the responses to the IoTSRM2-based survey by organization category, industry sector, and region" [Pop+21b].

Thus, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.6 shows "the percentage distribution of the survey respondents by position level, which reveals that the majority of the survey respondents (i.e., 84%) correspond to and are evenly distributed across" the "C-level executive and/or board member" and "Consulting practice leader and/or principal" position levels [Pop+21b]. Hence, "these two position levels of the survey respondents resulted in having the top percentage score for the surveyed organizations by survey respondents" [Pop+21b].

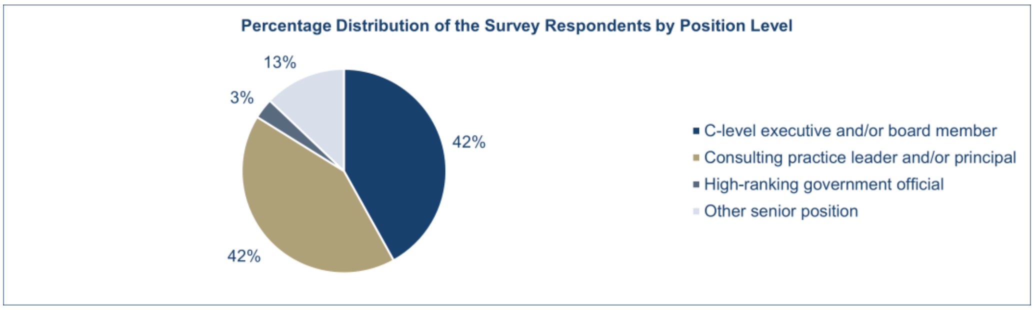


Fig. 6.6. Distribution of the survey respondents by position level [Pop+21b]

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.7 shows "the percentage distribution of the responses to the IoTSRM2-based survey by organization type (i.e., based on the organization size)" [Pop+21b]. In other words, "this figure shows the percentage distribution of the survey respondents' organizations of focus for this survey by organization category" [Pop+21b]. Hence, it reveals that the "Large Organization" category "makes up the greater part of the survey respondents' organizations of focus for this survey (i.e., the surveyed organizations)", which makes the "Large Organization" category "the top organization type by survey respondents for the IoTSRM2-based survey" [Pop+21b]. It is worth noting that "these organizations of focus may indicate the organizations or client organizations of the survey respondents depending on what they were referring to when completing the IoTSRM2-based survey" [Pop+21b].

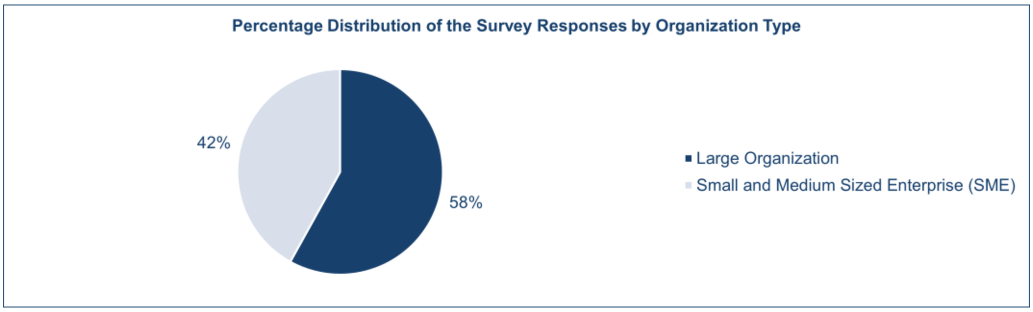


Fig. 6.7. Distribution of survey responses by organization category [Pop+21b]

Then, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.8 presents "the percentage distribution of the responses to the IoTSRM2-based survey by industry classification" [Pop+21b]. In other words, "this figure shows the percentage distribution of the survey respondents' organizations or client organizations by industry sector" [Pop+21b]. Hence, it reveals that the "Technology, Media, & Telecom (TMT)" industry sector "makes up the top industry sector for the survey respondents' organizations of focus for this survey (i.e., the surveyed organizations)" [Pop+21b].

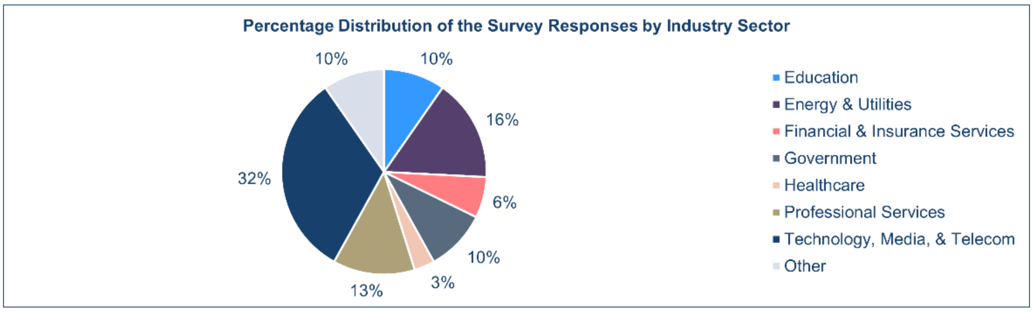


Fig. 6.8. Distribution of survey responses by industry classification [Pop+21b]

Then, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.9 shows "the percentage distribution of the organizations of focus of the survey respondents for this survey by region, which reveals that the majority of the responses to the IoTSRM2-based survey (i.e., around 81%) correspond to organizations headquartered in" the "Europe, Middle East and Africa (EMEA)" and "North/South America" regions [Pop+21b]. Moreover, it is worth noting that the "North/South America" region "resulted in having the top percentage score for the surveyed organizations by survey respondents" [Pop+21b].

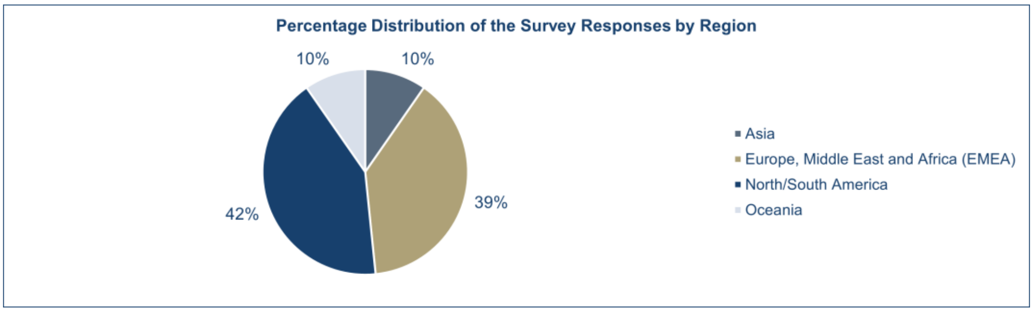


Fig. 6.9. Distribution of the survey responses by region [Pop+21b]

6.3.1.2 Results for Part II of the IoTSRM2-Based Survey

Based on the information disseminated by the author through the research paper [Pop+21b], Chapter 6.3.1.2 "provides the main results for part II of this IoTSRM2-based survey, including the results on the IoTSRM2 controls along with the weighted results on the IoTSRM2 controls and on the entire IoTSRM2 for the surveyed organizations" [Pop+21b].

Results on IoTSRM2 Controls for Surveyed Organizations

First, based on the information disseminated by the author through the research paper [Pop+21b], Chapter 6.3.1.2 "outlines the key results on the IoTSRM2 controls for the survey respondents' organizations or client organizations (i.e., the surveyed organizations) by showing the IoTSRM2 view for the survey responses to the IoTSRM2-related questions" [Pop+21b].

Thus, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.10 provides "the IoTSRM2 view for the survey responses to the IoTSRM2-related questions and highlights for each IoTSRM2 control and related question the overall tendency of the corresponding survey responses (i.e., towards either deviating from or meeting the as-is IoTSRM2 control in question)" [Pop+21b]. This figure aims "to allow readers to rapidly pinpoint, for each IoTSRM2 control and related question, how the majority of the survey respondents answered, specifically it enables readers to picture, for each IoTSRM2 control and related question, the concentrations of survey responses across two groups of answer choices" (i.e., "Yes, to a certain and great extent" and "No, to a certain and great extent") [Pop+21b]. A consolidated view of "the summary of the survey responses in numbers for each IoTSRM2-related question and IoTSRM2 control is provided in Appendix A3 as part of Table A3.1" which includes "the number of survey responses corresponding to each answer choice for the IoTSRM2-related questions" [Pop+21b].

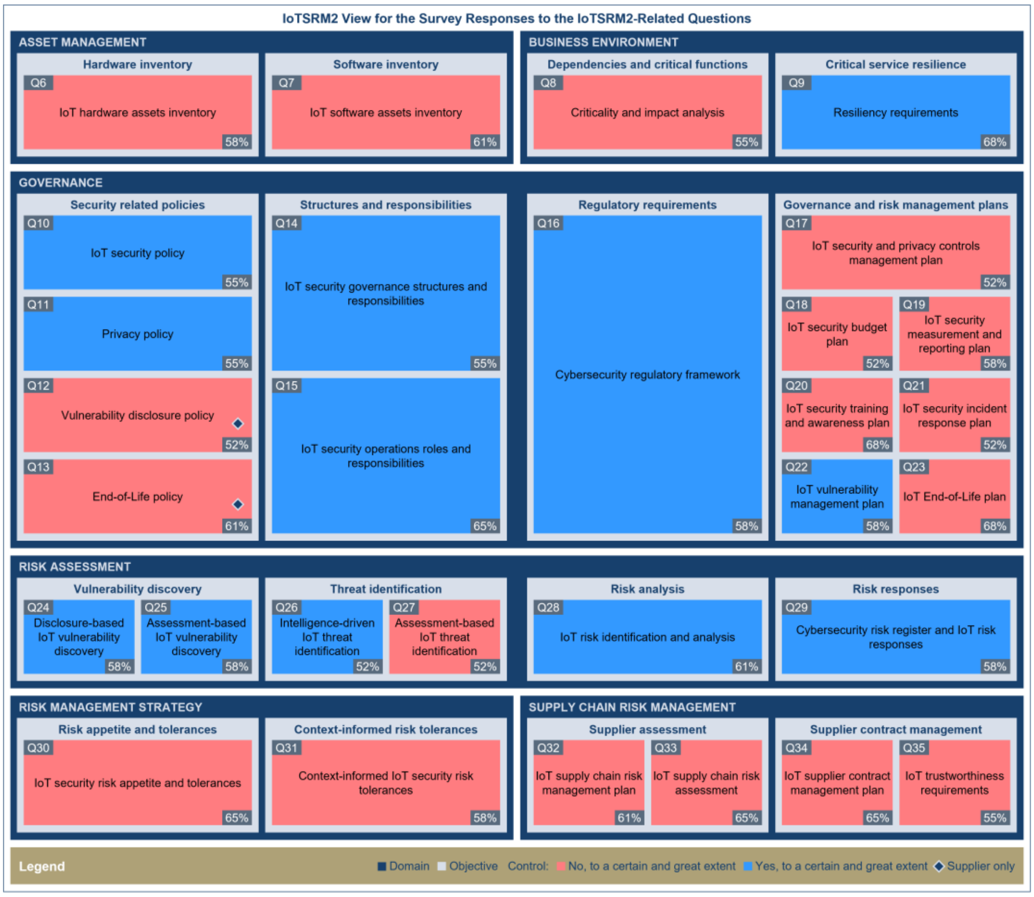

IoTSRM2 View for the Survey Responses to the IoTSRM2-Related Questions
ASSET MANAGEMENT
Hardware inventory
Q6
IoT hardware assets inventory
58%
Software inventory
Q7
IoT software assets inventory
61%
BUSINESS ENVIRONMENT
Dependencies and critical functions
Q8
Criticality and impact analysis
55%
Critical service resilience
Q9
Resiliency requirements
68%
GOVERNANCE
Security related policies
Q10
IoT security policy
55%
Q11
Privacy policy
55%
Q12
Vulnerability disclosure policy
52%
Q13
End-of-Life policy
61%
Structures and responsibilities
Q14
IoT security governance structures and responsibilities
55%
Q15
IoT security operations roles and responsibilities
65%
Regulatory requirements
Q16
Cybersecurity regulatory framework
58%
Governance and risk management plans
Q17
IoT security and privacy controls management plan
52%
Q18
IoT security budget plan
52%
Q19
IoT security measurement and reporting plan
58%
Q20
IoT security training and awareness plan
68%
Q21
IoT security incident response plan
52%
Q22
IoT vulnerability management plan
58%
Q23
IoT End-of-Life plan
68%
RISK ASSESSMENT
Vulnerability discovery
Q24
Disclosure-based IoT vulnerability discovery
58%
Q25
Assessment-based IoT vulnerability discovery
58%
Threat identification
Q26
Intelligence-driven IoT threat identification
52%
Q27
Assessment-based IoT threat identification
52%
Risk analysis
Q28
IoT risk identification and analysis
61%
Risk responses
Q29
Cybersecurity risk register and IoT risk responses
58%
RISK MANAGEMENT STRATEGY
Risk appetite and tolerances
Q30
IoT security risk appetite and tolerances
65%
Context-informed risk tolerances
Q31
Context-informed IoT security risk tolerances
58%
SUPPLY CHAIN RISK MANAGEMENT
Supplier assessment
Q32
IoT supply chain risk management plan
61%
Q33
IoT supply chain risk assessment
65%
Supplier contract management
Q34
IoT supplier contract management plan
65%
Q35
IoT trustworthiness requirements
55%
Legend
■ Domain □ Objective Control: ■ No, to a certain and great extent ■ Yes, to a certain and great extent ◆ Supplier only

Fig. 6.10. IoTSRM2 overview for the responses to the IoTSRM2-based survey [Pop+21b]

First, with respect to the "Yes, to a certain and great extent" group of answer choices from Fig. 6.10, "this group corresponds to and highlights each IoTSRM2 control and related question" for which "the percentage of survey responses" of "Yes, to a certain extent" and "Yes, to a great extent" of "the total number of survey responses for that IoTSRM2-related question" exceeds "the percentage of survey responses" of "No, to a great extent" and "No, to a certain extent" of "the total number of survey responses for that IoTSRM2-related question" [Pop+21b]. Hence, Fig. 6.10 shows that "the majority of survey respondents answered" either "Yes, to a certain extent" or "Yes, to a great extent" to the following "IoTSRM2-related questions" (i.e., "the question IDs in descending order by percentage of survey responses"): "Q9", "Q15", "Q28", "Q16", "Q22", "Q24", "Q25", "Q29", "Q10", "Q11", "Q14", and "Q26" [Pop+21b].

Then, about the "No, to a certain and great extent" group of answer choices, "this group corresponds to and highlights each IoTSRM2 control and related question" for which "the percentage of survey responses" of "No, to a great extent" and "No, to a certain extent" of "the total number of survey responses for that IoTSRM2-related question" exceeds "the percentage of survey responses" of "Yes, to a certain extent" and "Yes, to a great extent" of "the total number of survey responses for that IoTSRM2-related question" [Pop+21b]. Hence, Fig. 6.10 shows that "the majority of survey respondents answered" either "No, to a great extent" or "No, to a certain extent" to the following "IoTSRM2-related questions" (i.e., "the question IDs in descending order by percentage of survey responses"): "Q20", "Q23", "Q34", "Q33", "Q30", "Q32", "Q13", "Q7", "Q31", "Q19", "Q6", "Q35", "Q8", "Q27", "Q21", "Q18", "Q17", and "Q12" [Pop+21b].

Therefore, "considering where the heavy concentrations of the survey responses are across the two groups of answer choices for each IoTSRM2 control and related question, the majority of the surveyed organizations resulted in having the highest performance in" the "Risk Assessment" and "Business Environment" domains, in that order, whereas "the majority of the surveyed organizations resulted in having the lowest performance in" the "Asset Management", "Risk Management Strategy", "Supply Chain Risk Management", and "Governance" domains, in that order [Pop+21b].

First, with respect to the "Risk Assessment" domain, except for the "Assessment-based IoT threat identification" control, "the majority of the survey responses" are "Yes, to a certain extent" and "Yes, to a great extent" for the corresponding "IoTSRM2" controls (i.e., "Disclosure-based IoT vulnerability discovery", "Assessment-based IoT vulnerability discovery", "Intelligence-driven IoT threat identification", "IoT risk identification and analysis", and "Cybersecurity risk register and IoT risk responses") and related questions [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], this result shows that, "although most of the surveyed organizations are not so preoccupied with undertaking comprehensive IoT threat profiling exercises, these organizations do engage in IoT risk assessments" [Pop+21b].

Second, about the "Business Environment" domain, while "most of the survey responses" are "No, to a great extent" and "No, to a certain extent" for the "Criticality and impact analysis" control and related question, "most of the survey responses" for the "Resiliency requirements" control and related question are "Yes, to a certain extent" and "Yes, to a great extent" [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], on the one hand, "the finding suggests that most of the surveyed organizations are not so preoccupied with prioritizing IoT related assets based on their criticality to the organization, which may indicate that most surveyed organizations adopt one-size-fits-all approaches in defending IoT enabled services and enablers" [Pop+21b]. On the other hand, "the finding shows that the majority of the surveyed organizations are very preoccupied with improving the resilience of their IoT infrastructures, which may suggest that most surveyed organizations focus on securing their IoT infrastructure resilience to compensate for their intake of IoT security and privacy risks" [Pop+21b].

Then, with respect to the "Asset Management" domain, "the majority of survey responses" are "No, to a great extent" and "No, to a certain extent" for both corresponding "IoTSRM2" controls (i.e., "IoT hardware assets inventory" and "IoT software assets inventory") and related questions [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], this result shows that "most of the surveyed organizations lack all-encompassing IoT asset inventories, which may exacerbate shadow IoT in these organizations and diversify the unknown attack vectors for these organizations" [Pop+21b].

Afterwards, with respect to the "Risk Management Strategy" domain, "the majority of survey responses" are "No, to a great extent" and "No, to a certain extent" for both corresponding "IoTSRM2" controls (i.e., "IoT security risk appetite and tolerances" and "Context-informed IoT security risk tolerances") and related questions [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], this finding suggests that "most surveyed organizations adopt either one-size-fits-all or ad hoc approaches in managing their IoT security and privacy risks which may drive deep disproportionalities or inefficiencies and inconsistencies in the execution of their IoT security risk management strategies, respectively" [Pop+21b].

Subsequently, with respect to the "Supply Chain Risk Management" domain, "the majority of survey responses" are "No, to a great extent" and "No, to a certain extent" for all four corresponding "IoTSRM2" controls (i.e., "IoT supply chain risk management plan", "IoT supply chain risk assessment", "IoT supplier contract management plan", and "IoT trustworthiness requirements") and related questions [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], this finding reveals that "most surveyed organizations underperform when it comes to managing IoT supply chain risk which may increase the likelihood of IoT supply chain risk occurrence given that IoT adoption amplifies the interdependencies between the surveyed organizations and their supply chains" [Pop+21b]. This is because "they tend to manage their relationships with their IoT suppliers in an ad hoc fashion rather than relying on structured IoT supply chain risk assessments and trustworthiness requirements underpinned by clearly defined IoT supply chain risk management and IoT supplier contract management plans" [Pop+21b].

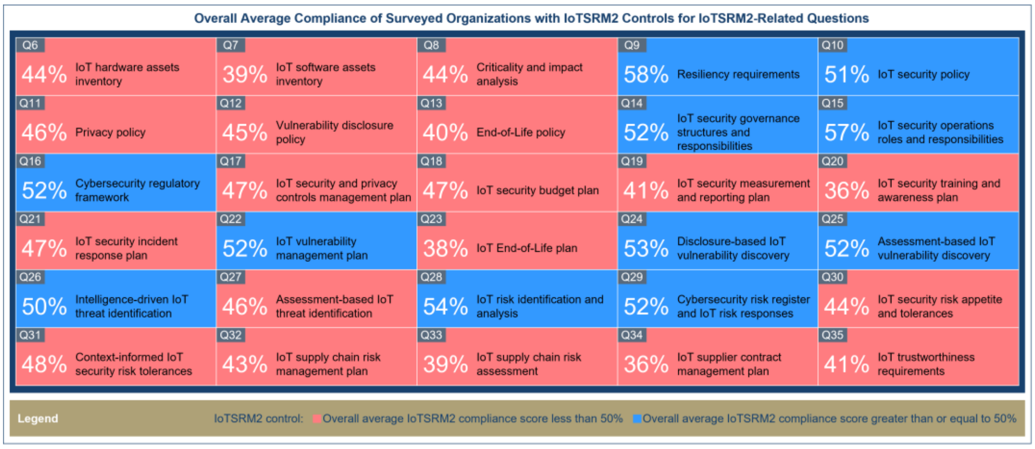
As for the "Governance" domain, based on the information disseminated by the author through the research paper [Pop+21b], "the majority of the survey responses" are "Yes, to a certain extent" and "Yes, to a great extent" for the "IoT security policy", "Privacy policy", "IoT security operations roles and responsibilities", "IoT security governance structures and responsibilities", "Cybersecurity regulatory framework", and "IoT vulnerability management plan" controls and related questions, whereas "the majority of the survey responses" are "No, to a great extent" and "No, to a certain extent" for the "Vulnerability disclosure policy", "End-of-Life policy", "IoT security and privacy controls management plan", "IoT security budget plan", "IoT security measurement and reporting plan", "IoT security training and awareness plan", "IoT security incident response plan", and "IoT End-of-Life plan" controls and related questions [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], this finding suggests that "although most surveyed organizations have IoT security and privacy policies, understand their compliance obligations, and have IoT security governance structures and responsibilities in place, they underperform in strategizing governance and risk management for their IoT infrastructures (i.e., except for vulnerability management) and fail in ensuring that their IoT suppliers have clearly documented vulnerability disclosure and End-of-Life policies in place" [Pop+21b]. Hence, "considering that the majority of the surveyed organizations may rely on a relatively fragile base for crafting their IoT security risk management strategy, this finding is quite worrying for these organizations as it may have cascading consequences on the execution of their IoT security risk management strategy" [Pop+21b].

In this context, "the majority of the surveyed organizations should consider reviewing and improving their controls related to the IoTSRM2 controls" of the "Asset Management", "Risk Management Strategy", "Supply Chain Risk Management", and "Governance" domains [Pop+21b].

Weighted Results on IoTSRM2 Controls for Surveyed Organizations

Second, based on the information disseminated by the author through the research paper [Pop+21b], Chapter 6.3.1.2 "outlines the key results on the IoTSRM2 controls for the surveyed organizations by outlining the overall average compliance with IoTSRM2 controls" [Pop+21b]. Thus, "the overall average IoTSRM2 compliance score for each IoTSRM2 control and related question resulted based on all survey responses and the corresponding IoTSRM2 adjusted control weight for that IoTSRM2 control and related question" [Pop+21b]. It is worth noting that, "for each IoTSRM2 control, the overall average IoTSRM2 compliance score is calculated using Equations (6.1), (6.2) and (6.3)" (see Chapter 6.2.3) [Pop+21b].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.11 presents "the consolidated view of the survey responses through the corresponding overall average IoTSRM2 compliance score for each IoTSRM2 control and related question" [Pop+21b]. For each IoTSRM2 control and related question, this figure indicates "whether the corresponding overall average IoTSRM2 compliance score leans towards deviating from or meeting the as-is IoTRSM2 control" [Pop+21b].



Overall Average Compliance of Surveyed Organizations with IoTSRM2 Controls for IoTSRM2-Related Questions

Q6 44% IoT hardware assets inventory	Q7 39% IoT software assets inventory	Q8 44% Criticality and impact analysis	Q9 58% Resiliency requirements	Q10 51% IoT security policy
Q11 46% Privacy policy	Q12 45% Vulnerability disclosure policy	Q13 40% End-of-Life policy	Q14 52% IoT security governance structures and responsibilities	Q15 57% IoT security operations roles and responsibilities
Q16 52% Cybersecurity regulatory framework	Q17 47% IoT security and privacy controls management plan	Q18 47% IoT security budget plan	Q19 41% IoT security measurement and reporting plan	Q20 36% IoT security training and awareness plan
Q21 47% IoT security incident response plan	Q22 52% IoT vulnerability management plan	Q23 38% IoT End-of-Life plan	Q24 53% Disclosure-based IoT vulnerability discovery	Q25 52% Assessment-based IoT vulnerability discovery
Q26 50% Intelligence-driven IoT threat identification	Q27 46% Assessment-based IoT threat identification	Q28 54% IoT risk identification and analysis	Q29 52% Cybersecurity risk register and IoT risk responses	Q30 44% IoT security risk appetite and tolerances
Q31 48% Context-informed IoT security risk tolerances	Q32 43% IoT supply chain risk management plan	Q33 39% IoT supply chain risk assessment	Q34 36% IoT supplier contract management plan	Q35 41% IoT trustworthiness requirements

Legend IoTSRM2 control: 🟥 Overall average IoTSRM2 compliance score less than 50% 🟦 Overall average IoTSRM2 compliance score greater than or equal to 50%

Fig. 6.11. Overall average compliance with IoTSRM2 controls based on the survey responses [Pop+21b]

Based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.11 shows that "the overall average IoTSRM2 compliance score across the survey respondents' organizations or client organizations (i.e., the surveyed organizations) is less than 50% for the majority of the IoTSRM2 controls and only marginally greater than 50% for the remaining eleven IoTSRM2 controls" [Pop+21b]. Thus, based on the information disseminated by the author through the research paper [Pop+21b], the "Resiliency requirements", "IoT security operations roles and responsibilities", and "IoT risk identification and analysis" controls "resulted in having the top three highest overall average IoTSRM2 compliance scores, in that order", whereas the "IoT security training and awareness plan", "IoT supplier contract management plan", "IoT End-of-Life plan", "IoT software assets inventory", and "IoT supply chain risk assessment" controls "resulted in having the top three lowest overall average IoTSRM2 compliance scores, in that order" [Pop+21b].

First, "with respect to the top three highest overall average IoTSRM2 compliance scores", based on the information disseminated by the author through the research paper [Pop+21b], these findings suggest that "the majority of the surveyed organizations (i.e., the survey respondents' organizations or client organizations of focus for the IoTSRM2-based survey) concentrate on building security operations and resilience capabilities to withstand and recover rapidly from imminent cyber attacks, and they adopt a more proactive approach to address IoT security and privacy risks by leveraging IoT security risk assessments" [Pop+21b].

Second, with regard to the "IoT security training and awareness plan" control, the survey result shows that "the majority of the surveyed organizations lack the as-is IoTSRM2 control on the IoT security training and awareness" [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], this finding of the survey suggests that "most surveyed organizations are not well informed on or do not clearly understand the IoT security and privacy risks they face, which may lead them to being more susceptible to poor formulation and/or execution of IoT security risk management strategies which may in turn lead to unsecure IoT technology adoption, usage of unsecure IoT technologies, and propagation of cyber attacks due to not knowing whether their IoT infrastructure is breached or where and how to rapidly report suspicious/unusual IoT activity" [Pop+21b].

Then, with respect to the "IoT supplier contract management plan" control, the survey finding reveals that "the majority of the surveyed organizations deviate or nearly deviate from the as-is corresponding IoTSRM2 control" [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], this result of the survey shows that "most surveyed organizations may be exposed to heightened levels of IoT supply chain risk due to engaging in ad hoc rather than well planned IoT supply chain risk management practices that might omit dealing with certain IoT supply chain risks and in effect fail to provide an adequate level of defense against nefarious or security negligent third party entities" [Pop+21b].

With respect to the "IoT End-of-Life plan" control, the survey result reveals that "the majority of the surveyed organizations deviate or nearly deviate from the as-is corresponding IoTSRM2 control" [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], this result of the survey suggests that "most surveyed organizations are likely to end up using outdated and unsupported IoT technologies and having difficulties in adequately hardening their IoT technologies which would substantially increase their IoT attack surface in the long run" [Pop+21b].

Then, about the "IoT software assets inventory" control, the survey result reveals that "the majority of the surveyed organizations deviate or nearly deviate from the as-is corresponding IoTSRM2 control" [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], this finding of the survey suggests that "most surveyed organizations may already experience different extents of shadow IoT software, which for some of them may be way beyond their IoT security risk appetites without knowing it" [Pop+21b].

As for the "IoT supply chain risk assessment" control, the survey result shows that "the majority of the surveyed organizations deviate or nearly deviate from the as-is corresponding IoTSRM2 control" [Pop+21b]. Based on the information disseminated by the author through the research paper [Pop+21b], this finding of the survey suggests that "most surveyed organizations do not actively assess their IoT supply chain risks across several supply chain tiers, which may not only hinder their ability to adequately enforce a base level of trust across their supply chain but also diminish their ability to rapidly identify and mitigate the IoT security-related risks stemming from their supply chain" [Pop+21b].

In this context, "the majority of surveyed organizations should consider fast-tracking the improvement of their capabilities related to" the "IoT security training and awareness plan", "IoT supplier contract management plan", "IoT End-of-Life plan", "IoT software assets inventory", and "IoT supply chain risk assessment" controls of "IoTSRM2" [Pop+21b]. Moreover, "to allow for better prioritization of effort, the surveyed organizations should consider improving these capabilities in tandem with their capabilities related to" the "Criticality and impact analysis" of the "IoTSRM2" [Pop+21b].

Weighted Results on IoTSRM2 for Surveyed Organizations

Then, based on the information disseminated by the author through the research paper [Pop+21b], Chapter 6.3.1.2 "provides the key results on the entire IoTSRM2 for the surveyed organizations by outlining the degree of compliance of each of these organizations with the IoTSRM2" [Pop+21b]. "The IoTSRM2 compliance score for each surveyed organization resulted based on all survey responses of that surveyed organization and the IoTSRM2 adjusted control weights for each of the IoTSRM2 controls and related questions" [Pop+21b]. It is worth noting that "the IoTSRM2 compliance score for each surveyed organization is calculated using Equation (6.4)" (see Chapter 6.2.3) [Pop+21b].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], "for each of the surveyed organizations from each of the four regions of the world considered in the IoTSRM2-based survey", Fig. 6.12 "shows the corresponding IoTSRM2 compliance score and indicates whether this score is less than 50% or greater than or equal to 50%" [Pop+21b]. It is worth noting that "each surveyed organization is uniquely identified using the proposed naming convention (see Chapter 6.2.3) which allows readers to differentiate surveyed organizations from each other and to determine the organization category and industry classification of each surveyed organization from its name" [Pop+21b].

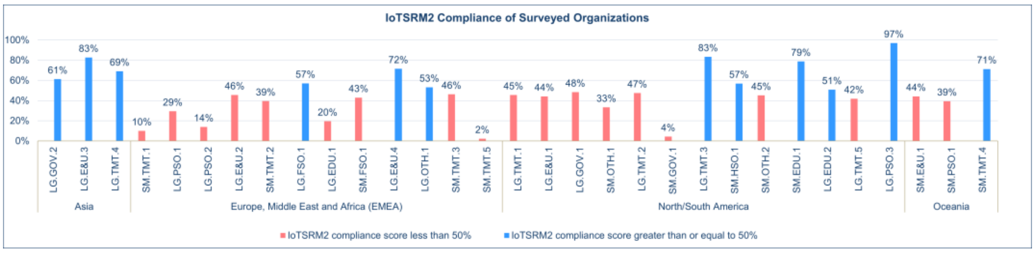


Fig. 6.12. The IoTSRM2 compliance of surveyed organizations [Pop+21b]

Thus, based on the information disseminated by the author through the research paper [Pop+21b], "the top three highest IoTSRM2 compliance scores correspond to one large organization (i.e., LG.PSO.3) from the North/South America region, one large organization (i.e., LG.E&U.3) from the Asia region, one large organization (i.e., LG.TMT.3) from the North/South America region, and one small-medium organization (i.e., SM.EDU.1) from the North/South America region, in that order", whereas "the top three lowest IoTSRM2 compliance scores correspond to one small-medium organization (i.e., SM.TMT.5) from the Europe, Middle East and Africa (EMEA) region, one small-medium organization (i.e., SM.GOV.1) from the North/South America region, and one small-medium organization (i.e., SM.TMT.1) from the Europe, Middle East and Africa (EMEA) region, in that order" [Pop+21b]. "About the surveyed organizations that have the top three highest IoTSRM2 compliance scores", these results show that "except for LG.E&U.3, all organizations are from the North/South America region" [Pop+21b]. Moreover, "except for SM.EDU.1, all surveyed organizations that have the top three highest IoTSRM2 compliance scores are large organizations" [Pop+21b]. "As for the surveyed organizations that have the top three lowest IoTSRM2 compliance scores", these results show that "except for SM.GOV.1, all organizations are from the Europe, Middle East and Africa (EMEA) region" [Pop+21b]. Moreover, "all surveyed organizations that have the top three lowest IoTSRM2 compliance scores are small-medium organizations" [Pop+21b].

Furthermore, "when it comes to the IoTSRM2 compliance scores across all industry sectors and regions", based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.12 shows that "half of the surveyed large organizations (i.e., LG.PSO.3, LG.TMT.3, LG.E&U.3, LG.E&U.4, LG.TMT.4, LG.GOV.2, LG.FSO.1, LG.OTH.1, and LG.EDU.2) scored greater than or equal to 50%", whereas "most surveyed small-medium organizations (i.e., SM.TMT.5, SM.GOV.1, SM.TMT.1, SM.OTH.1, SM.PSO.1, SM.TMT.2, SM.FSO.1, SM.E&U.1, SM.OTH.2, and SM.TMT.3) scored less than 50%" [Pop+21b].

Then, "with respect to the IoTSRM2 compliance scores for the surveyed large organizations for each industry sector irrespective of their region", based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.12 reveals the following [Pop+21b]:

- "Half of the surveyed organizations for the Energy & Utilities industry sector (i.e., LG.E&U.3 and LG.E&U.4) scored greater than or equal to 50%" [Pop+21b];
- "Half of the surveyed organizations for the Education industry sector (i.e., LG.EDU.2) scored greater than or equal to 50%" [Pop+21b];
- "All surveyed organizations for the Financial & Insurance Services industry sector (i.e., LG.FSO.1) scored greater than or equal to 50%" [Pop+21b];
- "Half of the surveyed organizations for the Government industry sector (i.e., LG.GOV.2) scored greater than or equal to 50%" [Pop+21b];
- "All surveyed organizations for the Other industry sector (i.e., LG.OTH.1) scored greater than or equal to 50%" [Pop+21b];
- "Most surveyed organizations for the Professional Services industry sector (i.e., LG.PSO.1 and LG.PSO.2) scored less than 50%" [Pop+21b];
- "Most surveyed organizations for the Technology, Media, & Telecom industry sector (i.e., LG.TMT.2, LG.TMT.1, and LG.TMT.5) scored less than 50%" [Pop+21b].

Hence, "considering the percentage of surveyed large organizations that scored IoTSRM2 compliance greater than or equal to 50% for each industry sector irrespective of their region, the surveyed large organizations for the Financial & Insurance Services and Other industry sectors scored higher than those corresponding to the remaining industry sectors" [Pop+21b].

"About the IoTSRM2 compliance scores for the surveyed small-medium organizations for each industry sector irrespective of their region", based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.12 reveals the following [Pop+21b]:

- "All surveyed organizations for the Energy & Utilities industry sector (i.e., SM.E&U.1) scored less than 50%" [Pop+21b];

- "All surveyed organizations for the Education industry sector (i.e., SM.EDU.1) scored greater than or equal to 50%" [Pop+21b];
- "All surveyed organizations for the Financial & Insurance Services industry sector (i.e., SM.FSO.1) scored less than 50%" [Pop+21b];
- "All surveyed organizations for the Government industry sector (i.e., SM.GOV.1) scored less than 50%" [Pop+21b];
- "All surveyed organizations for the Healthcare industry sector (i.e., SM.HSO.1) scored greater than or equal to 50%" [Pop+21b];
- "All surveyed organizations for the Other industry sector (i.e., SM.OTH.2 and SM.OTH.1) scored less than 50%" [Pop+21b];
- "All surveyed organizations for the Professional Services industry sector (i.e., SM.PSO.1) scored less than 50%" [Pop+21b];
- "Most surveyed organizations for the Technology, Media, & Telecom industry sector (i.e., SM.TMT.3, SM.TMT.2, SM.TMT.1, and SM.TMT.5) scored less than 50%" [Pop+21b].

Hence, "considering the percentage of surveyed small-medium organizations that scored IoTSRM2 compliance greater than or equal to 50% for each industry sector irrespective of their region, the surveyed organizations for the Education and Healthcare industry sectors scored higher than those corresponding to the other industry sectors" [Pop+21b].

Furthermore, "with respect to the IoTSRM2 compliance scores for the surveyed large organizations for each region regardless of their industry sector", based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.12 shows the following [Pop+21b]:

- "All surveyed organizations for the Asia region (i.e., LG.E&U.3, LG.TMT.4, and LG.GOV.2) scored greater than or equal to 50%" [Pop+21b];
- "Most surveyed organizations for the Europe, Middle East and Africa (EMEA) region (i.e., LG.E&U.2, LG.PSO.1, LG.EDU.1, and LG.PSO.2) scored less than 50%" [Pop+21b];
- "Most surveyed organizations for the North/South America region (i.e., LG.GOV.1, LG.TMT.2, LG.TMT.1, LG.E&U.1, and LG.TMT.5) scored less than 50%" [Pop+21b].

Hence, "percentage-wise, more surveyed large organizations regardless of their industry sector scored IoTSRM2 compliance greater than or equal to 50% for the Asia region than for each of the other regions" [Pop+21b].

"As for the IoTSRM2 compliance scores for the surveyed small-medium organizations for each region regardless of their industry sector", based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.12 shows the following [Pop+21b]:

- "All surveyed organizations for the Europe, Middle East and Africa (EMEA) region (i.e., SM.TMT.3, SM.FSO.1, SM.TMT.2, SM.TMT.1, and SM.TMT.5) scored less than 50%" [Pop+21b];
- "Most surveyed organizations for the North/South America region (i.e., SM.OTH.2, SM.OTH.1, and SM.GOV.1) scored less than 50%" [Pop+21b];
- "Most surveyed organizations for the Oceania region (i.e., SM.E&U.1 and SM.PSO.1) scored less than 50%" [Pop+21b].

Thus, "percentage-wise, more surveyed small-medium organizations regardless of their industry sector scored IoTSRM2 compliance greater than or equal to 50% for the North/South America region than for each of the other regions" [Pop+21b].

6.3.2. Results for Surveyed Large Organizations

This sub-subchapter is structured in three sub-subsubchapters. Based on the information disseminated by the author through the research paper [Pop+21b], first "it provides the results for part I of the IoTSRM2-based survey on the surveyed large organizations", second "it provides the results for part II of the IoTSRM2-based survey on the surveyed large organizations", and then "it provides the survey results on the surveyed large organizations that operate in the Technology, Media, & Telecom (TMT) industry sector" [Pop+21b].

6.3.2.1 Results for Part I of the IoTSRM2-Based Survey on Surveyed Large Organizations

Based on the information disseminated by the author through the research paper [Pop+21b], Chapter 6.3.2.1 "provides the main results for part I of the IoTSRM2-based survey on the surveyed large organizations (i.e., the top organization type by surveyed organizations) including the percentage distribution of the survey respondents for large organizations by position level and the percentage distributions of the responses to the IoTSRM2-based survey for large organizations by industry sector and regions" [Pop+21b].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.13 provides "the percentage distribution of the survey respondents for surveyed large organizations by position level", which reveals that the "Consulting practice leader and/or principal" position level "makes up the majority of the survey respondents for large organizations (i.e., around 56%)", followed by the "C-level executive and/or board member" position level [Pop+21b]. Hence, the "Consulting practice leader and/or principal" position level of the survey respondents "resulted in having the top percentage score for the surveyed large organizations by survey respondents" [Pop+21b].

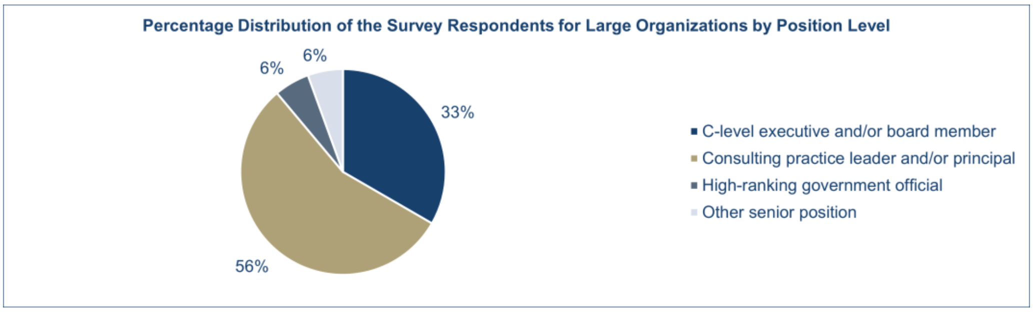


Fig. 6.13. Distribution of the survey respondents for large organizations by position level [Pop+21b]

Then, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.14 shows "the percentage distribution of the survey responses for surveyed large organizations by industry classification" [Pop+21b]. Hence, this figure reveals that the "Technology, Media, & Telecom (TMT)" industry sector "makes up the top industry sector for the surveyed large organizations" [Pop+21b].

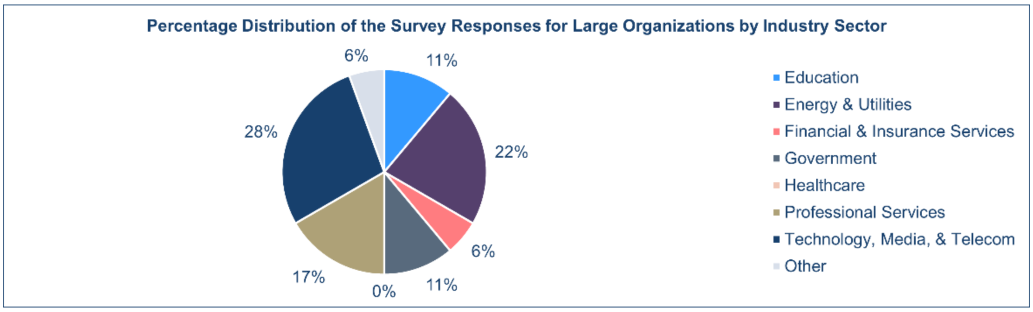


Fig. 6.14. Distribution of survey responses for large organizations by industry classification [Pop+21b]

Then, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.15 shows "the percentage distribution of the surveyed large organizations by region, which reveals that most survey responses (i.e., 83%) correspond to organizations headquartered in" the "North/South America" and "Europe, Middle East and Africa (EMEA)" regions [Pop+21b]. Thus, the "North/South America" region "resulted in having the top percentage score (i.e., 44%) for the surveyed large organizations by survey respondents" [Pop+21b].

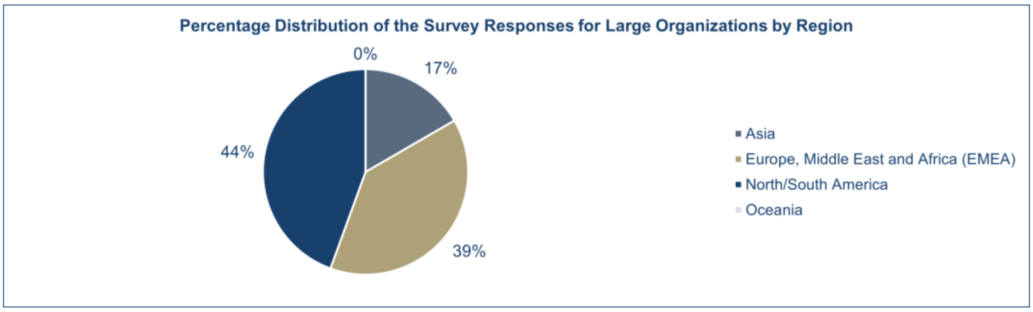


Fig. 6.15. Distribution of survey responses for large organizations by region [Pop+21b]

6.3.2.2 Results for Part II of the IoTSRM2-Based Survey on Surveyed Large Organizations

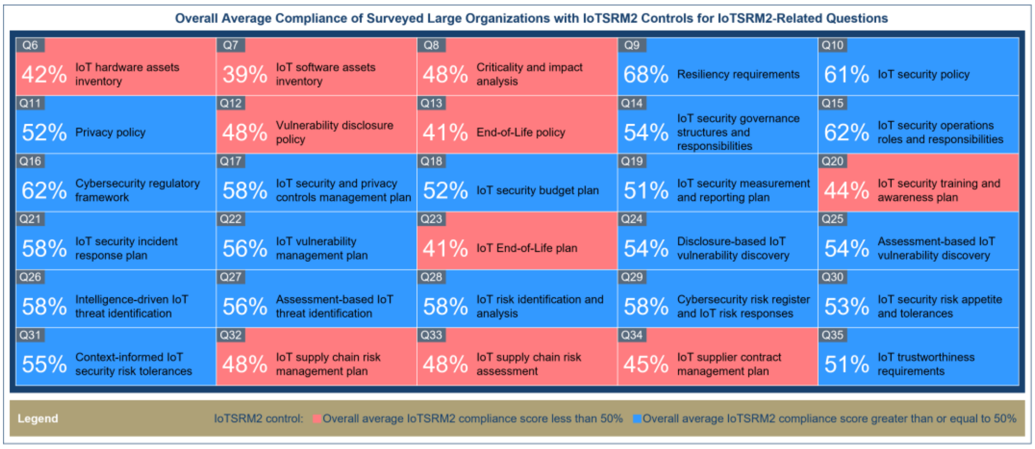
Based on the information disseminated by the author through the research paper [Pop+21b], Chapter 6.3.2.2 "provides the main results for part II of the

IoTSRM2-based survey on the surveyed large organizations, including the weighted results on IoTSRM2 controls for the surveyed large organizations" [Pop+21b].

Weighted results on IoTSRM2 controls for surveyed large organizations

Based on the information disseminated by the author through the research paper [Pop+21b], Chapter 6.3.2.2 "outlines the key results on the IoTSRM2 controls for the surveyed large organizations by outlining the overall average compliance with IoTSRM2 controls" [Pop+21b]. "The overall average IoTSRM2 compliance score for each IoTSRM2 control and related question resulted based on all survey responses for surveyed large organizations and the corresponding IoTSRM2 adjusted control weight for that IoTSRM2 control and related question" [Pop+21b]. It is worth noting that, "for each IoTSRM2 control, the overall average IoTSRM2 compliance score is calculated using Equations (6.1), (6.2) and (6.3)" (see Chapter 6.2.3) [Pop+21b].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.16 presents "the consolidated view of the survey responses on the surveyed large organizations through the corresponding overall average IoTSRM2 compliance score for each IoTSRM2 control and related question" [Pop+21b]. "For each IoTSRM2 control and related question", this figure indicates "whether the corresponding overall average IoTSRM2 compliance score leans towards deviating from or meeting the as-is IoTRSM2 control" [Pop+21b].



Overall Average Compliance of Surveyed Large Organizations with IoTSRM2 Controls for IoTSRM2-Related Questions

Q6 🟥 42% IoT hardware assets inventory	Q7 🟥 39% IoT software assets inventory	Q8 🟥 48% Criticality and impact analysis	Q9 🟦 68% Resiliency requirements	Q10 🟦 61% IoT security policy
Q11 🟦 52% Privacy policy	Q12 🟥 48% Vulnerability disclosure policy	Q13 🟥 41% End-of-Life policy	Q14 🟦 54% IoT security governance structures and responsibilities	Q15 🟦 62% IoT security operations roles and responsibilities
Q16 🟦 62% Cybersecurity regulatory framework	Q17 🟦 58% IoT security and privacy controls management plan	Q18 🟦 52% IoT security budget plan	Q19 🟦 51% IoT security measurement and reporting plan	Q20 🟥 44% IoT security training and awareness plan
Q21 🟦 58% IoT security incident response plan	Q22 🟦 56% IoT vulnerability management plan	Q23 🟥 41% IoT End-of-Life plan	Q24 🟦 54% Disclosure-based IoT vulnerability discovery	Q25 🟦 54% Assessment-based IoT vulnerability discovery
Q26 🟦 58% Intelligence-driven IoT threat identification	Q27 🟦 56% Assessment-based IoT threat identification	Q28 🟦 58% IoT risk identification and analysis	Q29 🟦 58% Cybersecurity risk register and IoT risk responses	Q30 🟦 53% IoT security risk appetite and tolerances
Q31 🟦 55% Context-informed IoT security risk tolerances	Q32 🟥 48% IoT supply chain risk management plan	Q33 🟥 48% IoT supply chain risk assessment	Q34 🟥 45% IoT supplier contract management plan	Q35 🟦 51% IoT trustworthiness requirements

Legend IoTSRM2 control: 🟥 Overall average IoTSRM2 compliance score less than 50% 🟦 Overall average IoTSRM2 compliance score greater than or equal to 50%

Fig. 6.16. Overall average compliance with IoTSRM2 controls based on the survey responses for large organizations [Pop+21b]

Based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.16 shows that "the overall average IoTSRM2 compliance score across the surveyed large organizations is marginally greater than 50% for the majority of the IoTSRM2 controls and less than 50% for the remaining ten IoTSRM2 controls" [Pop+21b]. Thus, the "Resiliency requirements", "IoT security operations roles and responsibilities", "Cybersecurity regulatory framework" and "IoT security policy" controls "resulted in having the top three highest overall average IoTSRM2 compliance scores, in that order", whereas the "IoT software assets inventory", "IoT End-of-Life plan", "End-of-Life policy", and "IoT hardware assets inventory" controls "resulted in having the top three lowest overall average IoTSRM2 compliance scores, in that order" [Pop+21b].

First, "with respect to the top three highest overall average IoTSRM2 compliance scores", based on the information disseminated by the author through the research paper [Pop+21b], these findings suggest that "the majority of the surveyed large organizations focus on building more resilient mission critical IoT enabled services, maintain clearly defined IoT security operations roles and responsibilities, are aware of their IoT security and privacy regulatory obligations, and have their top management's commitment towards IoT security articulated through a formal IoT security policy" [Pop+21b].

Second, "regarding the top and fourth lowest overall average IoTSRM2 compliance scores", namely for the "IoT software assets inventory" and "IoT hardware assets inventory" controls, respectively, based on the information disseminated by the author through the research paper [Pop+21b], the survey results show that "the majority of the surveyed large organizations do not have a comprehensive situational awareness on their IoT assets" [Pop+21b]. This finding is quite worrying as it suggests that "the majority of the surveyed large organizations not only they do not know their whole IoT attack surface but also may not have a clear picture of their cyber threat landscape, which may negatively impact their ability to adequately assess and manage their IoT security and privacy risks and in turn affect their ability to adequately protect their IoT infrastructures and enabled assets" [Pop+21b].

"As for the second and third lowest overall average IoTSRM2 compliance scores", namely for the "IoT End-of-Life plan" and "End-of-Life policy" controls, respectively, based on the information disseminated by the author through the research paper [Pop+21b], the survey results show that "the majority of the surveyed large organizations deviate or nearly deviate from the as-is corresponding IoTSRM2 controls" [Pop+21b]. These findings of the survey suggest that "the majority of the surveyed large organizations are sitting on a time bomb relative to their IoT adoptions" [Pop+21b]. This is because of "the security and privacy implications of ending up relying on End-of-Life IoT assets without proper in-house planning in advance and awareness of their IoT suppliers' sunsetting plans" [Pop+21b]. These implications range from having "unsecured hackable IoT assets lying around" to "experiencing life-threatening IoT failures" [Pop+21b].

Thus, "the majority of surveyed large organizations should consider accelerating the improvement of their capabilities related to" the "IoT software assets inventory", "IoT hardware assets inventory", "IoT End-of-Life plan", and "End-of-Life policy" controls of "IoTSRM2" [Pop+21b]. Moreover, "to allow for better prioritization of effort, the surveyed large organizations should consider improving these capabilities in tandem with their capabilities related to" the "Criticality and impact analysis" of the "IoTSRM2" [Pop+21b].

6.3.2.3 Results for Surveyed Large Organizations from Technology, Media, & Telcom (TMT)

Based on the information disseminated by the author through the research paper [Pop+21b], Chapter 6.3.2.3 "first provides the main results for part I of the IoTSRM2-based survey on the surveyed large organizations that operate in the Technology, Media, & Telecom (TMT) industry sector and then it provides the results for part II of the IoTSRM2-based survey on the surveyed large TMT organizations, which focuses on the weighted results on IoTSRM2 controls for the surveyed large TMT organizations" [Pop+21b].

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

First, based on the information disseminated by the author through the research paper [Pop+21b], Chapter 6.3.2.3 "provides the percentage distribution of the survey respondents for large TMT organizations by position level and the percentage distribution of the survey responses for large TMT organizations by region" [Pop+21b].

Thus, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.17 provides "the percentage distribution of the survey respondents for large TMT organizations by position level, which shows that the majority of the survey respondents for large TMT organizations (i.e., 80%) correspond to and are evenly distributed across" the "C-level executive and/or board member" and "Consulting practice leader and/or principal" position levels [Pop+21b]. Thus, "these two position levels of the survey respondents resulted in having the top percentage score for the surveyed large TMT organizations by survey respondents" [Pop+21b].

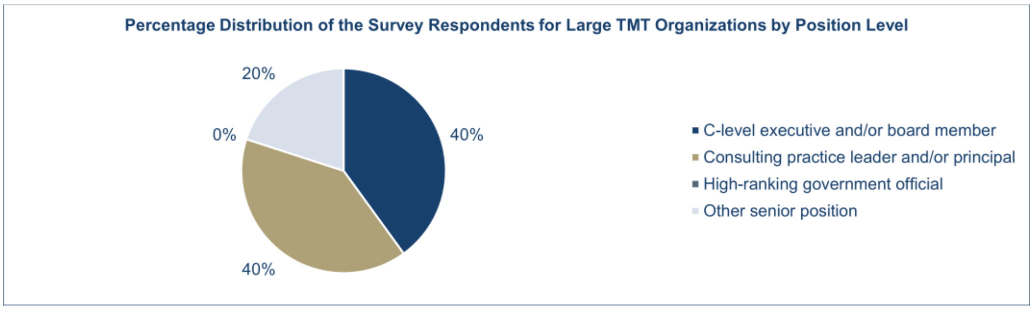


Fig. 6.17. Distribution of the survey respondents for large TMT organizations by position level [Pop+21b]

Then, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.18 shows "the percentage distribution of the surveyed large TMT organizations by region, which reveals that most survey responses for large TMT organizations (i.e., 80%) correspond to organizations headquartered in" the "North/South America" region [Pop+21b]. Hence, the "North/South America" region "resulted in having the top percentage score for the surveyed large TMT organizations by survey respondents" [Pop+21b].

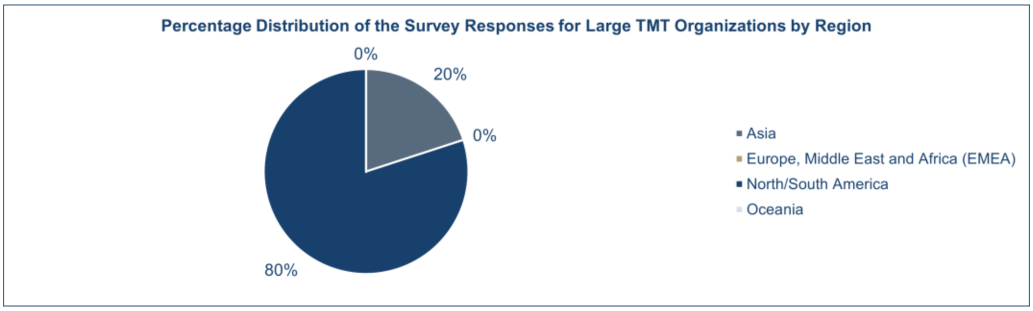
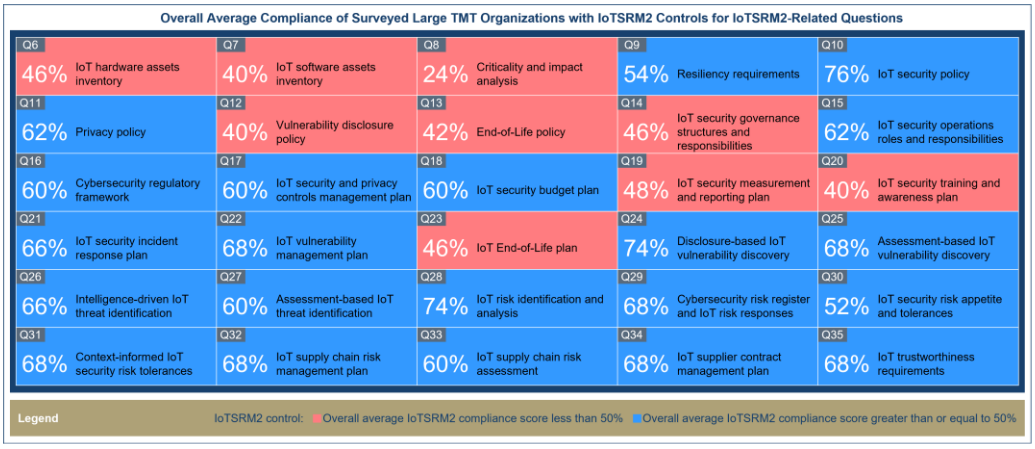


Fig. 6.18. Distribution of survey responses for large TMT organizations by region [Pop+21b]

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

Second, based on the information disseminated by the author through the research paper [Pop+21b], Chapter 6.3.2.3 "outlines the key results on the IoTSRM2 controls for the surveyed large TMT organizations by outlining the overall average compliance with IoTSRM2 controls" [Pop+21b]. "The overall average IoTSRM2 compliance score for each IoTSRM2 control and related question resulted based on all survey responses for surveyed large TMT organizations and the corresponding IoTSRM2 adjusted control weight for that IoTSRM2 control and related question" [Pop+21b]. It is worth noting that, "for each IoTSRM2 control, the overall average IoTSRM2 compliance score is calculated using Equations (6.1), (6.2) and (6.3)" (see Chapter 6.2.3) [Pop+21b].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.19 presents "the consolidated view of the survey responses on the surveyed large TMT organizations through the corresponding overall average IoTSRM2 compliance score for each IoTSRM2 control and related question" [Pop+21b]. "For each IoTSRM2 control and related question", this figure indicates "whether the corresponding overall average IoTSRM2 compliance score leans towards deviating from or meeting the as-is IoTRSM2 control" [Pop+21b].


Overall Average Compliance of Surveyed Large TMT Organizations with IoTSRM2 Controls for IoTSRM2-Related Questions

Q6 46% IoT hardware assets inventory	Q7 40% IoT software assets inventory	Q8 24% Criticality and impact analysis	Q9 54% Resiliency requirements	Q10 76% IoT security policy
Q11 62% Privacy policy	Q12 40% Vulnerability disclosure policy	Q13 42% End-of-Life policy	Q14 46% IoT security governance structures and responsibilities	Q15 62% IoT security operations roles and responsibilities
Q16 60% Cybersecurity regulatory framework	Q17 60% IoT security and privacy controls management plan	Q18 60% IoT security budget plan	Q19 48% IoT security measurement and reporting plan	Q20 40% IoT security training and awareness plan
Q21 66% IoT security incident response plan	Q22 68% IoT vulnerability management plan	Q23 46% IoT End-of-Life plan	Q24 74% Disclosure-based IoT vulnerability discovery	Q25 68% Assessment-based IoT vulnerability discovery
Q26 66% Intelligence-driven IoT threat identification	Q27 60% Assessment-based IoT threat identification	Q28 74% IoT risk identification and analysis	Q29 68% Cybersecurity risk register and IoT risk responses	Q30 52% IoT security risk appetite and tolerances
Q31 68% Context-informed IoT security risk tolerances	Q32 68% IoT supply chain risk management plan	Q33 60% IoT supply chain risk assessment	Q34 68% IoT supplier contract management plan	Q35 68% IoT trustworthiness requirements

Legend IoTSRM2 control: 🟥 Overall average IoTSRM2 compliance score less than 50% 🟦 Overall average IoTSRM2 compliance score greater than or equal to 50%

Fig. 6.19. Overall average compliance with IoTSRM2 controls based on the survey responses for large TMT organizations [Pop+21b]

Based on the information disseminated by the author through the research paper [Pop+21b], Fig. 6.19 shows that "the overall average IoTSRM2 compliance score across the surveyed large TMT organizations is greater than 50% for the majority of the IoTSRM2 controls and less than 50% for the other nine IoTSRM2 controls" [Pop+21b]. Hence, the "IoT security policy", "Disclosure-based IoT vulnerability discovery", "IoT risk identification and analysis", "IoT vulnerability management plan", "Assessment-based IoT vulnerability discovery", "Context-informed IoT security risk tolerances", "IoT trustworthiness requirements", "Cybersecurity risk register and IoT risk responses", "IoT supply chain risk management plan", and "IoT supplier contract management plan" controls "resulted in having the top three highest overall average IoTSRM2 compliance scores, in that order", whereas the "Criticality and impact analysis", "Vulnerability disclosure policy", "IoT software assets inventory", and "IoT security training and awareness plan" controls "resulted in having the top three lowest overall average IoTSRM2 compliance scores, in that order" [Pop+21b].

First, "with respect to the top three highest overall average IoTSRM2 compliance scores", based on the information disseminated by the author through the research paper [Pop+21b], the survey results reveal that "the majority of the surveyed large TMT organizations have their senior management's commitment towards IoT security clearly articulated through a formal IoT security policy, adopt proactive risk assessment approaches fueled by IoT vulnerability management, and understand the importance of maintaining their preparedness for facing IoT supply chain risk related events" [Pop+21b].

Then, about the "Criticality and impact analysis" control, the survey result reveals that "most surveyed large TMT organizations deviate or nearly deviate from the as-is corresponding IoTSRM2 control" [Pop+21b]. Thus, based on the information disseminated by the author through the research paper [Pop+21b], "although most of the surveyed large TMT organizations adopt proactive risk assessment approaches", this survey result suggests that "many or at least some of these organizations address IoT risks in most cases using one-size-fits-all IoT security risk management approaches which could have catastrophic consequences" [Pop+21b]. For instance, based on the information disseminated by the author through the research paper [Pop+21b], "catastrophic consequences could turn up in the event of a life-threatening IoT risk occurrence while having implemented hugely disproportionate countermeasures across the board to effectively address this IoT risk" [Pop+21b].

With respect to the "Vulnerability disclosure policy" control, based on the information disseminated by the author through the research paper [Pop+21b], "although the majority of the surveyed large TMT organizations engage in IoT supply chain risk management", the finding shows that "most of these organizations contract IoT suppliers that either do not have an up-to-date vulnerability disclosure policy or do not communicate it well enough to them" [Pop+21b]. Moreover, "considering that most surveyed large TMT organizations leverage vulnerability disclosures as part of their risk assessment processes", this survey finding further suggests that "these organizations establish vulnerability handling processes with their IoT suppliers ahead of contracting" [Pop+21b]. Notwithstanding, "the absence of a publicly available vulnerability disclosure policy may translate for these large TMT organizations in not being able to avail of timely IoT patches and in turn having unpatched hackable IoT technologies in use due to lags in third party IoT vulnerability reporting" [Pop+21b].

Furthermore, with respect to the "IoT software assets inventory" control, based on the information disseminated by the author through the research paper [Pop+21b], the survey result shows that "the majority of the surveyed large TMT organizations do not have an all-encompassing picture of all their IoT software assets, which further indicates that these organizations may be exposed to shadow IoT software" [Pop+21b]. Moreover, "considering that the survey finding shows that some of these organizations are also unaware of all their IoT hardware assets, these large TMT organizations should consider better dealing with inventorying their IoT assets to reduce the likelihood of bad thinks happening" [Pop+21b]. It is worth noting that, based on the information disseminated by the author through the research paper [Pop+21b], "shadow IoT risk may have a cascading effect on the performance of the IoT risk assessment processes if it materializes" [Pop+21b].

As for the "IoT security training and awareness plan" control, the survey result reveals that "most of the surveyed large organizations deviate or nearly deviate from the as-is corresponding IoTSRM2 control" [Pop+21b]. This survey finding suggests that "the majority of the surveyed large TMT organizations are unaware of or do not clearly grasp their IoT security and privacy risks, which in turn may favor scenarios where these organizations are breached due to lack of IoT risk awareness" [Pop+21b].

Thus, "the majority of the surveyed large TMT organizations should consider boosting the pace of the improvement of their capabilities related to" the "Criticality and impact analysis", "Vulnerability disclosure policy", "IoT software assets inventory", and "IoT security training and awareness plan" controls of the "IoTSRM2" [Pop+21b].

6.4. Related Work

Based on the information disseminated by the author through the research papers [Pop+21a] and [Pop+21b], "a sizeable number of academic and industry research studies has been published on IoT security" [Pop+21a], [Pop+21b]. However, at the time of writing, "no research study was found to exclusively focus on determining the current state of IoT security risk management strategies in organizations" [Pop+21b]. Hence, based on the information disseminated by the author through the research paper [Pop+21b], "given there are numerous research studies in the literature relevant to IoT security", this chapter "encompasses the related work to the IoTSRM2-related survey study and covers the related works that meet the following three selection criteria and one condition" [Pop+21b]:

- **"Selection criterion 1":** "The related work is available in English" [Pop+21b];
- **"Selection criterion 2":** "The related work is focused on determining the current state of IoT security risk management strategy in organizations at least to a certain extent" [Pop+21b];
- **"Selection criterion 3":** "The related work employs an interview-, survey-, or experiment-based research method" [Pop+21b];
- **"Condition 1":** "The related works are research studies from both academia and industry" [Pop+21b].

Thus, based on the information disseminated by the author through the research paper [Pop+21b], Table 6.8 "lists the 12 selected related works for the evaluation, and it outlines the following details": "the current row number" (i.e., "No."), "the author/publisher of the related research study" (i.e., "Author/Publisher"), "the title of the research work" (i.e., "Title"), and "the corresponding reference" (i.e., "Reference") [Pop+21b].

Table 6.8. Selected related works [Pop+21b]

No.	Author/Publisher	Title	Reference
1.	"Almutairi and Almarhabi"	"Investigation of Smart Home Security and Privacy: Consumer Perception in Saudi Arabia"	[Alm+21]
2.	"Arm Limited"	"Bridging the Gap PSA Certified Security Report 2021 How collaboration will secure the future of IoT"	[Arm21]
3.	"Asplund and Nadjm-Tehrani"	"Attitudes and Perceptions of IoT Security in Critical Societal Services"	[Asp+16]
4.	"Forescout Technologies"	"The Enterprise of Things Security Report The State of IoT Security"	[For21]
5.	"Gemalto"	"The State of IoT Security"	[Gem18]
6.	"IBM"	"Electronics Industrial IoT cybersecurity"	[IBM18b]
7.	"Juniper Networks and Internet of Things Institute"	"Securing IoT at Scale Requires a Holistic Approach Survey Insights Revealed by IoT Adopters"	[Jun+18]
8.	"Palo Alto Networks"	"2020 Unit 42 IoT Threat Report"	[Pal20]
9.	"The Cabinet Office"	"Consumer Attitudes Towards IoT Security"	[Cab20]
10.	"The Ponemon Institute"	"A New Roadmap for Third Party IoT Risk Management the Critical Need to Elevate Accountability, Authority and Engagement"	[Pon20]
11.	"The SANS Institute"	"The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns"	[SAN18]
12.	"UL"	"Security concerns escalate as IoT expands Market insights on the state of IoT security"	[UL19]

Then, based on the information disseminated by the author through the research paper [Pop+21b], this subchapter "covers the analysis of the 12 selected related works" [Pop+21b]. Thus, "with respect to the analysis of the literature related to the IoTSRM2-based survey study", based on the information disseminated by the author through the research paper [Pop+21b], Table 6.9 shows "the IoTSRM2-based survey study together with the 12 reviewed related works mapped against the proposed evaluation criteria and the extent of applicability to each evaluation criterion" [Pop+21b]. With respect to the proposed evaluation criteria, "seven evaluation criteria were formulated based on the proposed methodology for determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2" [Pop+21b] (see Chapter 6.2). Moreover, with respect to the extent of applicability, "three types of applicability were considered relevant to indicate differences and/or similarities between this IoTSRM2-based survey study and the in-scope research works for this evaluation" [Pop+21b].

Table 6.9. The IoTSRM2-based survey study and related work mapped to evaluation criteria and extent of applicability [Pop+21b]

	Extent of Applicability		
Evaluation Criterion	**The Evaluation Criterion Fully Applies**	**The Evaluation Criterion Applies to a Certain Extent**	**The "as-is" Evaluation Criterion Does Not Apply**
"E1: The research study is focused on determining the current state of IoT security risk management strategies in organizations" [Pop+21b]	"The IoTSRM2-based survey study"	[Alm+21], [Arm21], [Asp+16], [Cab20], [For21], [Gem18], [IBM18b], [Jun+18], [Pal20], [Pon20], [SAN18], [UL19]	"None of these related works"
"E2: The methodology for achieving the intended purpose of the research study is clearly described" [Pop+21b]	[For21], "The IoTSRM2-based survey study"	[Alm+21], [Arm21], [Asp+16], [Cab20], [Pal20]	[Gem18], [IBM18b], [Jun+18], [Pon20], [SAN18], [UL19]
"E3: The underlying design best practice of the research method of the methodology, is clearly documented" [Pop+21b]	"The IoTSRM2-based survey study"	[Asp+16]	[Alm+21], [Arm21], [Cab20], [For21], [Gem18], [IBM18b], [Jun+18], [Pal20], [Pon20], [SAN18], [UL19]
"E4: Provides results for organizations of a specific organization size" [Pop+21b]	[Arm21], [Gem18], [SAN18], "The IoTSRM2-based survey study"	"None of these related works"	[Alm+21], [Asp+16], [Cab20], [For21], [IBM18b], [Jun+18], [Pal20], [Pon20], [UL19]
"E5: Provides results for organizations from a specific industry sector" [Pop+21b]	[For21], [IBM18b], [Pal20], [UL19], "The IoTSRM2-based survey study"	"None of these related works"	[Alm+21], [Arm21], [Asp+16], [Cab20], [Gem18], [Jun+18], [Pon20], [SAN18]
"E6: The results reveal the level of compliance of each subject with a reference model" [Pop+21b]	"The IoTSRM2-based survey study"	[SAN18]	[Alm+21], [Arm21], [Asp+16], [Cab20], [For21], [Gem18], [IBM18b], [Jun+18], [Pal20], [Pon20], [UL19]
"E7: The findings resemble the results of the IoTSRM2-based survey" [Pop+21b]	"The IoTSRM2-based survey study"	[Arm21], [Gem18], [IBM18b], [Jun+18], [Pal20], [Pon20], [SAN18], [UL19]	[Alm+21], [Asp+16], [Cab20], [For21]

Afterwards, based on the information disseminated by the author through the research paper [Pop+21b], this chapter presents "the evaluation of this IoTSRM2-based survey study and the 12 reviewed related works for each evaluation criterion" [Pop+21b].

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

Based on the information disseminated by the author through the research paper [Pop+21b], "none of the reviewed related works focused on determining the current state of IoT security risk management strategies in organizations" [Pop+21b]. However, "the 12 reviewed related works addressed this issue to a certain extent by focusing on determining the current state of IoT security in organizations (i.e., [Arm21], [Asp+16], [For21], [Gem18], [Jun+18], [Pal20], [UL19]), of Industrial IoT (IIoT) security in organizations (i.e., [IBM18b], [SAN18]), of IoT security for consumers (i.e., [Alm+21], [Cab20]) and of third party IoT risk management in organizations (i.e., [Pon20])" [Pop+21b].

"With respect to the seven reviewed related works that focused on determining the current state of IoT security in organizations", based on the information disseminated by the author through the research paper [Pop+21b], these related works "focused their studies on understanding IoT security challenges and opportunities, threats, risks, capabilities and enablers, and investment priorities" [Pop+21b]. Thus, first, Arm Limited (2021) [Arm21] "focused their study on understanding the IoT security challenges and opportunities from the surveyed organizations" [Pop+21b]. Second, Asplund and Nadjm-Tehrani (2016) [Asp+16] "investigated the attitudes and perceptions among interviewed industry actors on IoT security in critical societal services" [Pop+21b]. Third, Forescout Technologies (2021) [For21] "provided the state of enterprise IoT network security of some of their customer deployments within and across industry verticals by looking at enterprise network threat and risk exposure" [Pop+21b]. Fourth, Gemalto (2018) [Gem18] "provided the IoT security state in surveyed organizations by looking at the IoT security capabilities of and the use of blockchain technology to secure IoT data, services, and devices in surveyed organizations" [Pop+21b]. Then, "as part of the Juniper Networks white paper on IoT security", Juniper Networks and Internet of Things Institute (2018) [Jun+18] "reported on the IoT security risks, challenges, capabilities, and investment priorities of surveyed organizations that have implemented IoT projects" [Pop+21b]. Afterwards, Palo Alto Networks (2020) [Pal20] "evaluated the state of the IoT threat landscape by using data from real deployments" [Pop+21b]. Finally, UL (2019) [UL19] "focused their survey study on determining how the organizations are preparing for and responding to the current and emerging IoT security threats" [Pop+21b].

Then, based on the information disseminated by the author through the research paper [Pop+21b], "about the two reviewed related works that focused on determining the current state of IIoT security in organizations", IBM (2018b) [IBM18b] "determined the IIoT security risks and their implications for the surveyed organizations from the energy and industrial sectors", and the SANS Institute (2018) [SAN18] "investigated the capabilities, threats, and risks of IIoT security in surveyed organizations" [Pop+21b].

"With respect to the two reviewed related works that focused on determining the current state of IoT security for consumers", based on the information disseminated by the author through the research paper [Pop+21b], Almutairi and

Almarhabi (2021) [Alm+21] "studied the security and privacy concerns of their survey respondents about the smart home devices in the Saudi Arabia", and the Cabinet Office (2020) [Cab20] "investigated the consumer attitudes towards IoT security" [Pop+21b].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], the Ponemon Institute (2020) [Pon20] "focused on determining the current state of third party IoT risk management in surveyed organizations" [Pop+21b].

"Compared with these 12 reviewed related works", the "IoTSRM2-based survey study" is focused on "determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2" [Pop+21b].

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

"The proposed three-phased methodology for achieving the intended purpose of this IoTSRM2-based survey study, namely determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2", is clearly described (see Chapter 6.2) [Pop+21b]. "The proposed methodology includes nine steps and outputs related to" the "Plan and Create", "Launch and Run", and "Analyze and Report" phases [Pop+21b].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], "from the 12 reviewed related works, one of them clearly described the methodology used for achieving the intended purpose of the research study (i.e., [For21]), five of them partially described their methodology (i.e., [Alm+21], [Arm21], [Asp+16], [Cab20], [Pal20]), while the remaining ones did not describe their methodology (i.e., [Gem18], [IBM18b], [Jun+18], [Pon20], [SAN18], [UL19])" [Pop+21b].

"Regarding the related work that clearly described its methodology", based on the information disseminated by the author through the research paper [Pop+21b], Forescout Technologies (2021) [For21] "provided the methodology applied for determining the state of enterprise IoT network security of some of their customer deployments by outlining three main steps, namely data collection, data cleaning and enrichment, and data analysis" [Pop+21b]. Furthermore, Forescout Technologies (2021) [For21] "provided details about the risk score model created and used to measure the risk values for all IoT devices of some of their customer deployments, which were then used to analyze the anonymous enterprise device data from the Forescout Device Cloud" [Pop+21b]. In contrast with the research work performed by Forescout Technologies (2021) [For21] which "entails an experimental study that processes data from some of their customer deployments", the proposed methodology from this chapter "involves a survey-based study that leverages the survey data drawn from the survey respondents on the surveyed organizations" [Pop+21b]. Although "the proposed methodology from this chapter has different objectives than the study conducted by Forescout Technologies (2021) [For21]", similar to the methodology of Forescout Technologies [For21] which "includes among others, data collection, data cleaning, and data analysis steps for anonymous data", the proposed three-phased methodology "includes, among others, steps that entail the collection, cleaning and analysis of anonymous data as part of the launch and run, and analyze and report phases" [Pop+21b].

Furthermore, based on the information disseminated by the author through the research paper [Pop+21b], "from the perspective of the extent of applicability to this evaluation criterion", the proposed methodology "differentiates from the methodologies provided by Almutairi and Almarhabi (2021) [Alm+21], Arm Limited (2021) [Arm21], Asplund and Nadjm-Tehrani (2016) [Asp+16], the Cabinet Office (2020) [Cab20] and Palo Alto Networks (2020) [Pal20], as it is much more detailed than the ones of these five reviewed related works which offer limited details" [Pop+21b]. Thus, first, Almutairi and Almarhabi (2021) [Alm+21] "developed the questionnaire used for running the survey and provided details on how their questionnaire was developed" [Pop+21b]. However, Almutairi and Almarhabi (2021) [Alm+21] "provided limited details on how the survey planning and creation were performed and did not clearly outline the ways in which the analysis and reporting of survey responses were carried out" [Pop+21b]. Second, Arm Limited (2021) [Arm21] "provided limited details about their methodology including the use of the Sapio Research online panel for conducting the survey, the usage of email invitations, and the distribution channels used for requesting survey participation" [Pop+21b]. In this context, "the methodology provided by Arm Limited (2021) [Arm21] does not outline how the questionnaire is developed, how the survey is designed, and how the analysis and reporting of survey responses are performed" [Pop+21b]. Third, Asplund and Nadjm-Tehrani (2016) [Asp+16] "described the methodology for their interview-based study only half-way as it provides details about the type of questions used, the design of the questionnaire, the selection of the respondents, and the reporting format (i.e., through quotes) without describing the data collection and analysis activities" [Pop+21b]. Fourth, the Cabinet Office (2020) [Cab20] "provided limited details on their methodology and reported the use of the Ipsos MORI online panel for running their survey, the incentive used for attracting more survey participants, and the details concerning the request for survey participation" [Pop+21b]. However, the Cabinet Office (2020) [Cab20] "did not provide details on how the questionnaire was developed, how the survey was designed, and how the analysis and reporting of survey responses were performed" [Pop+21b]. Finally, Palo Alto Networks (2020) [Pal20] "provided merely some details about their experimental setup and data gathering rather than describing the analysis and reporting activities of the data collected from their customers" [Pop+21b].

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

As per Table 6.9 and based on the information disseminated by the author through the research paper [Pop+21b], "none of the 12 reviewed related works clearly documented the design best practice on which the research method of their methodology is based" [Pop+21b]. However, Asplund and Nadjm-Tehrani (2016) [Asp+16] "documented their own principles guiding the questionnaire design for their interview-based study, which are not based on a well renowned reference source" [Pop+21b]. "Compared with the 12 reviewed related works", the IoTSRM2-based survey study "relies on the principles for designing web questionnaires developed by Dillman et al. (1999) [Dil+99]", and "the applicability of these principles to the IoTSRM2-based survey is clearly documented" as part of Table 6.4 [Pop+21b].

"E4": "Provides results for organizations of a specific organization size"

Based on the information disseminated by the author through the research paper [Pop+21b], the "IoTSRM2-based survey study" reports "the percentage distribution of the surveyed organizations by organization category/type (i.e., based on the organization size) (see Chapter 6.3.1.1), the IoTSRM2 compliance score of each of the surveyed organizations together with indicating the category/type (i.e., based on size) of that organization (see Chapter 6.3.1.2), and the IoTSRM2-based survey results on the surveyed large organizations (see Chapter 6.3.2)" [Pop+21b].

In addition, “from the 12 reviewed related works, three of them provided results for organizations of a specific organization size (i.e., [Arm21], [Gem18], [SAN18]), whereas the remaining ones did not provide any results for organizations of a specific organization size (i.e., [Alm+21], [Asp+16], [Cab20], [For21], [IBM18b], [Jun+18], [Pal20], [Pon20], [UL19])” [Pop+21b].

“Regarding the three reviewed related works that provided results for organizations of a specific organization size”, based on the information disseminated by the author through the research paper [Pop+21b], Arm Limited (2021) [Arm21] “provided some of their results for small organizations and for large organizations (e.g., threat modelling adoption, satisfaction with IoT security expertise)”, Gemalto (2018) [Gem18] “provided all their results for large organizations having an employee headcount of more than 250”, and the SANS Institute (2018) [SAN18] “provided some of their results by organization size (e.g., number of connected IoT devices)” [Pop+21b].

“E5”: “Provides results for organizations from a specific industry sector”

Based on the information disseminated by the author through the research paper [Pop+21b], the “IoTSRM2-based survey study” provides “the percentage distribution of the surveyed organizations by industry classification/sector (see Chapter 6.3.1.1), the IoTSRM2 compliance score of each of the surveyed organizations together with indicating the industry sector of that organization (see Chapter 6.3.1.2), the percentage distribution of the surveyed large organizations by industry classification/sector (see Chapter 6.3.2.1), and the IoTSRM2-based survey results on the surveyed large TMT organizations (see Chapter 6.3.2.3)” [Pop+21b]. In addition, “from the 12 reviewed related works, four of them provided some of their survey results for organizations from a specific industry sector (i.e., [For21], [IBM18b], [Pal20], [UL19]), whereas the remaining ones did not provide any results for organizations from a specific industry sector (i.e., [Alm+21], [Arm21], [Asp+16], [Cab20], [Gem18], [Jun+18], [Pon20], [SAN18])” [Pop+21b].

“With respect to the four reviewed related works that provided results for organizations from a specific industry sector”, based on the information disseminated by the author through the research paper [Pop+21b], Forescout Technologies (2021) [For21] “provided all their findings for specific industry verticals”, IBM (2018b) [IBM18b] “provided all their results for the electronics industry sector”, Palo Alto Networks (2020) [Pal20] “provided their results for the enterprise IT and healthcare industry sectors and some of these results are mainly focused on the organizations from the healthcare industry sector”, and UL (2019) [UL19] “provided some of their results for organizations from specific industry sectors (e.g., IoT security plan)” [Pop+21b].

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

As per Table 6.9 and based on the information disseminated by the author through the research paper [Pop+21b], “none of the 12 reviewed related works provided results that reveal the level of compliance of the subjects with a reference model” [Pop+21b]. However, “the SANS Institute (2018) [SAN18] meets this evaluation criterion to a certain extent’ [Pop+21b]. This is because “the SANS Institute (2018) [SAN18] provided merely the overall results for their survey respondents, that indicate percentage scores of the IIoT devices connecting to different levels and zones of the network infrastructure following the Purdue model hierarchy rather than reporting the level of compliance of each subject with the Purdue model” [Pop+21b]. “Compared with the 12 reviewed related works”, the “IoTSRM2-

based survey study" outlines "the degree of compliance of each of the surveyed organizations with the IoTSRM2" (see Chapter 6.3.1.2) and provides "the IoTSRM2 compliance score for each of the surveyed organizations" (see Fig. 6.12) [Pop+21b].

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

Based on the information disseminated by the author through the research paper [Pop+21b], this chapter "provides the IoTSRM2-based survey results for each of the three groups of surveyed organizations (i.e., the surveyed large and small-medium organizations, the surveyed large organizations, and the surveyed large TMT organizations)" [Pop+21b]. As per Table 6.9, "none of the reviewed related works reported findings that fully resemble the results of the IoTSRM2-based survey" [Pop+21b]. However, "eight of the reviewed related works, namely Arm Limited (2021) [Arm21], Gemalto (2018) [Gem18], IBM (2018b) [IBM18b], Juniper Networks and Internet of Things Institute (2018) [Jun+18], Palo Alto Networks (2020) [Pal20], the Ponemon Institute (2020) [Pon20], the SANS Institute (2018) [SAN18], and UL (2019) [UL19], reported one or more findings that resemble some of the IoTSRM2-based survey results, while the remaining ones (i.e., [Alm+21], [Asp+16], [Cab20], [For21]) did not report any findings that resemble the IoTSRM2-based survey results" [Pop+21b].

"With respect to the eight reviewed related works that meet this evaluation criterion to a certain extent", based on the information disseminated by the author through the research paper [Pop+21b], "the Ponemon Institute (2020) [Pon20] reported five findings, Arm Limited (2021) [Arm21], Palo Alto Networks (2020) [Pal20], and the SANS Institute (2018) [SAN18] each reported four findings, Gemalto (2018) [Gem18] and IBM (2018b) [IBM18b] each reported two findings, and the remaining two research studies (i.e., [Jun+18], [UL19]) reported one finding that resemble some of the IoTSRM2-based survey results" [Pop+21b].

Hence, "with respect to the study conducted by the Ponemon Institute (2020) [Pon20], it reported five findings that resemble four of the weighted results of the IoTSRM2-based survey on the IoTSRM2 controls for the surveyed organizations" [Pop+21b] (see Chapter 6.3.1.2). First, "the long-term barrier reported by the Ponemon Institute (2020) [Pon20]", namely that "organizations should consider nurturing more robust risk cultures internally around their IoT environment", reflects "the IoTSRM2-based survey result related to" the "IoT security training and awareness plan" control of the "IoTSRM2" (see Fig. 6.11) [Pop+21b]. Second, "the finding reported by the Ponemon Institute (2020) [Pon20] that very few organizations actively engage in third party IoT security audits", is in line with "the IoTSRM2-based survey result on" the "IoT supplier contract management plan" control of the "IoTSRM2" (see Fig. 6.11) [Pop+21b]. Third, "the finding reported by the Ponemon Institute (2020) [Pon20] on IoT applications inventory", namely "the prevalent issue of maintaining a comprehensive and relevant inventory of IoT applications", reflects "the IoTSRM2-based survey result on" the "IoT software assets inventory" control of the "IoTSRM2" (see Fig. 6.11) [Pop+21b]. Finally, "the two findings reported by the Ponemon Institute (2020) [Pon20] on resource allocation", namely "the budget and staffing shortfalls to manage third party IoT risks", reflect "the IoTSRM2-based survey result on" the "IoT supply chain risk assessment" control of the "IoTSRM2" (see Fig. 6.11) [Pop+21b].

Then, "regarding the study conducted by Arm Limited (2021) [Arm21], it reported one finding that resembles one of the survey results on the IoTSRM2 controls for the surveyed organizations, one finding that resembles one of the survey results on the IoTSRM2 compliance score of each of the surveyed organizations, and two findings that somehow resemble one of the survey results on the IoTSRM2 controls for the surveyed organizations" [Pop+21b] (see Chapter 6.3.1.2). First, "the second top IoT security challenge reported by Arm Limited (2021) [Arm21]", namely "the lack of IoT security understanding and expertise", reflects "the IoTSRM2-based survey result related to" the "IoT security training and awareness plan" control of the "IoTSRM2" (see Fig. 6.10) [Pop+21b]. Second, "the finding reported by Arm Limited (2021) [Arm21] that IoT security implementation scales with the size of the organization", is in line with "the IoTSRM2-based survey finding that the top three highest and lowest IoTSRM2 compliance scores for the surveyed organizations correspond to large (i.e., except for one of them) and small-medium organizations, respectively" (see Fig. 6.12) [Pop+21b]. Third, "the findings reported by Arm Limited (2021) [Arm21] that the majority of their survey respondents (i.e., 53%) are not carrying out threat analysis for all the IoT products they provide and that nearly all of their survey respondents (i.e., 86%) are likely to do or redo the threat analysis in the postmarket phase of the IoT products they provide", are somehow related to "the IoTSRM2-based survey result on" the "Assessment-based IoT threat identification" control of the "IoTSRM2" in the context of "perhaps having surveyed organizations that work with IoT suppliers that are not so much engaged in performing thorough IoT threat profiling activities" (see Fig. 6.10) [Pop+21b].

Afterwards, "regarding the study carried out by Palo Alto Networks (2020) [Pal20], it reported four findings that resemble four of the survey results on the IoTSRM2 controls for the surveyed organizations" [Pop+21b] (see Chapter 6.3.1.2). First, "the finding reported by Palo Alto Networks (2020) [Pal20] that organizations lack IoT device inventory", is in line with "the IoTSRM2-based survey result on" the "IoT hardware assets inventory" control of the "IoTSRM2" (see Fig. 6.10) [Pop+21b]. Second, "the finding reported by the Palo Alto Networks (2020) [Pal20] that medical IoT devices run on outdated and End of Life operating systems", is in line with "the IoTSRM2-based survey result on" the "IoT End-of-Life plan" control of the "IoTSRM2" (see Fig. 6.10) [Pop+21b]. Third, "the finding reported by the Palo Alto Networks (2020) [Pal20] about the necessity of an effective IoT security strategy for managing IoT risk proactively", resembles "the IoTSRM2-based survey result that most of the surveyed organizations underperform in strategizing governance and risk management for their IoT infrastructures (i.e., except for vulnerability management)" (see Fig. 6.10) [Pop+21b]. Fourth, "the finding reported by the Palo Alto Networks (2020) [Pal20] that most organizations do not manage the risk profiles of their IoT devices", is somehow in line with "the IoTSRM2-based survey result that most of the surveyed organizations are not so much engaged in all-encompassing IoT threat profiling activities, which corresponds to" the "Assessment-based IoT threat identification" control of the "IoTSRM2" (see Fig. 6.10) [Pop+21b].

Then, "about the study conducted by the SANS Institute (2018) [SAN18], it reported two findings that resemble three of the survey results on the IoTSRM2 controls for the surveyed organizations, and two findings that somehow resemble two of the survey results on the IoTSRM2 controls for the surveyed organizations" [Pop+21b] (see Chapter 6.3.1.2). First, "the finding reported by the SANS Institute (2018) [SAN18] that most of their respondents (i.e., 59%), regardless of organization size, need additional education and training to manage security of IIoT devices", is in line with "the IoTSRM2-based survey result on" the "IoT security training and awareness plan" control of the "IoTSRM2" (see Fig. 6.10) [Pop+21b]. Second, "the finding reported by the SANS Institute (2018) [SAN18] that only 41.1% of their respondents have physical and logical inventory of connected devices to protect against IIoT risks", reflect "the IoTSRM2-based survey results on" the "IoT hardware assets inventory” and “IoT software assets inventory” controls of the “IoTSRM2” (see Fig. 6.10) [Pop+21b]. Third, “the top IIoT challenge reported by the SANS Institute (2018) [SAN18], namely the difficulty in or lack of patching for IIoT systems”, is somehow related to “the IoTSRM2-based survey result on” the “Vulnerability disclosure policy” control of the “IoTSRM2” from the perspective that “relying on an inadequate or absent vulnerability disclosure policy may favor scenarios where vulnerable IoT systems stay unpatched for longer periods of time” (see Fig. 6.10) [Pop+21b]. Fourth, “the third top IIoT challenge reported by the SANS Institute (2018) [SAN18], namely the difficulty in identifying and managing IIoT connectivity to critical infrastructure and other mission-critical systems”, is somehow related to “the IoTSRM2-based survey result on” the “Criticality and impact analysis” control of the “IoTSRM2” considering that “managing IoT interdependencies is cumbersome and inefficient without having all IoT enabled services and enablers prioritized based on their criticality” [Pop+21b].

Furthermore, “with respect to the study undertaken by Gemalto (2018) [Gem18], it reported one finding that resembles one of the survey results on the IoTSRM2 controls for the surveyed large organizations (see Chapter 6.3.2.1), and another that somehow resembles one of the weighted survey results on the IoTSRM2 controls for the surveyed large organizations (see Chapter 6.3.2.2)” [Pop+21b]. First, “considering that the organization size of all survey respondents of Gemalto (2018) [Gem18] is greater than 250 employees and corresponds to the surveyed large organizations of the IoTSRM2-based survey study (see Chapter 6.2)”, “the finding reported by Gemalto (2018) [Gem18] that the IT, Technology and Telecoms is the top organization sector by survey respondents”, reflects “the IoTSRM2-based survey result on the top industry sector for the surveyed large organizations by survey respondents, namely the Technology, Media, & Telecom (TMT) industry sector” (see Fig. 6.14) [Pop+21b]. Second, “the finding reported by Gemalto (2018) [Gem18] that the majority of their survey respondents that supply IoT products or services (i.e., 54%) increased their IoT security offerings”, is somehow related to “the IoTSRM2-based survey result on” the “IoT trustworthiness requirements” control of the “IoTSRM2” from the perspective that “having better IoT trustworthiness requirements for the IoT supplier contracts may demand and stimulate greater IoT security offerings on the supply side” (see Fig. 6.16) [Pop+21b].

Subsequently, “about the study performed by IBM (2018b) [IBM18b], it reported one finding that resembles one of the weighted survey results on the IoTSRM2 controls for the surveyed large TMT organizations, and another that somehow resembles and ramifies into three of the weighted survey results on the IoTSRM2 controls for the surveyed large TMT organizations” (see Chapter 6.3.2.3) [Pop+21b]. First, “the finding reported by IBM (2018b) [IBM18b] on the inventoried authorized and unauthorized IIoT software, reveals that under half of the majority of their surveyed electronics organizations control IoT software assets inventory”, and it reflects “the IoTSRM2-based survey result on” the “IoT software assets inventory” control of the “IoTSRM2” (see Fig. 6.19) [Pop+21b]. Second, “the finding reported by IBM (2018b) [IBM18b] on the secure IIoT devices, reveals that for virtually all their surveyed electronics organizations, engaging in continuous coordinated patching of IIoT devices is hard and very problematic when it comes to older legacy devices (e.g., End of Life legacy devices)”, and it somehow reflects “the IoTSRM2-based survey results on” the “Vulnerability disclosure policy”, “End-of-Life policy”, and “IoT End-of-Life plan” controls of the “IoTSRM2” considering that “the absence or the inadequacy of these three controls may have different repercussions on the organizations relying on them ranging from having unpatched and unsecure IoT devices to being hacked" (see Fig. 6.19) [Pop+21b].

Furthermore, "with respect to the study undertaken by Juniper Networks and Internet of Things Institute (2018) [Jun+18], it reported one finding that resembles one of the survey results on the IoTSRM2 controls for the surveyed organizations" [Pop+21b] (see Chapter 6.3.1.1). Hence, "the finding reported by Juniper Networks and Internet of Things Institute (2018) [Jun+18] that the Information Technology and Telecommunications industry sectors make up the top industry classification for their surveyed organizations", reflects "the IoTSRM2-based survey result on the top industry sector for the surveyed organizations by survey respondents, namely the Technology, Media, & Telecom (TMT) industry sector" (see Fig. 6.8) [Pop+21b].

Finally, "about the study conducted by UL (2019) [UL19], it reported one finding that resembles one of the survey results on the IoTSRM2 controls for the surveyed organizations" (see Chapter 6.3.1.2) [Pop+21b]. Hence, "the finding reported by UL (2019) [UL19] that the majority of their surveyed organizations (i.e., 77%) plan to increase spending in IoT security", is in line with "the IoTSRM2-based survey result on" the "IoT security budget plan" control of the "IoTSRM2" (see Fig. 6.10) [Pop+21b].

6.5. Conclusions

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

First, this chapter enumerated the research questions for the "IoTSRM2-based survey study" and provided a reading map for the research questions.

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

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

Hence, about “the results for all surveyed organizations”, first, these results revealed that the “C-level executive and/or board member” and “Consulting practice leader and/or principal” position levels are the top position levels of the survey respondents for these organizations. Second, the “IoTSRM2-based survey results” revealed that the “Large Organization” category is the top organization type for these organizations. Third, “IoTSRM2-based survey results” showed that the “Technology, Media, & Telecom (TMT)” industry sector is the top industry sector for these organizations. Fourth, these results showed that the “North/South America” region is the top region for these organizations. Fifth, about the overall tendency of the IoT security risk management strategies of these organizations relative to the “IoTSRM2” controls, the findings suggested, among others, that most organizations do best in the “Resiliency requirements” control and they do worst in the “IoT security training and awareness plan” and “IoT End-of-Life plan” controls. Then, about “the overall average IoTSRM2 compliance score” of these organizations for each “IoTSRM2” control, the findings showed, among others, that most organizations do best in the “Resiliency requirements” control and they do worst in the “IoT security training and awareness plan” and “IoT supplier contract management plan” controls. As for the “IoTSRM2 compliance score” of each of these organizations, the “IoTSRM2-based survey results” revealed, among others, that the top three highest and lowest “IoTSRM2 compliance scores” for the surveyed organizations correspond to large (i.e., except for one of them) and small-medium organizations, respectively.

Furthermore, about “the results for the surveyed large organizations”, first, these results revealed that the “Consulting practice leader and/or principal” position level is the top position level of the survey respondents for these organizations. Second, the “IoTSRM2-based survey results” showed that the “Technology, Media, & Telecom (TMT)” industry sector is the top industry sector for these organizations. Third, the “IoTSRM2-based survey results” showed that the “North/South America” region is the top region for these organizations. Fourth, about the “overall average IoTSRM2 compliance score” of these organizations for each “IoTSRM2” control, the findings showed, among others, that most organizations do best in the “Resiliency requirements” control and they do worst in the “IoT software assets inventory” control.

Furthermore, about “the results for the surveyed large TMT organizations”, first, the “IoTSRM2-based survey results” revealed that the “Consulting practice leader and/or principal” and “C-level executive and/or board member” position levels are the top position levels of the survey respondents for these organizations. Second, the findings showed that the “North/South America” region is the top region for these organizations. Third, about the “overall average IoTSRM2 compliance score” of these organizations for each “IoTSRM2” control, the “IoTSRM2-based survey results” showed, among others, that most organizations do best in the “IoT security policy” control and they do worst in the “Criticality and impact analysis” control.

Furthermore, this chapter outlined the related work. First, it highlighted the absence of research studies that exclusively focus on determining the current state of IoT security risk management strategies in organizations. Second, it selected 12 related research studies based on three selection criteria and one condition. Third, it discussed the “IoTSRM2-based survey study” in relation to the selected related studies using seven evaluation criteria based on the proposed methodology and using three types of applicability to each evaluation criterion. For instance, about the evaluation criterion on the research studies that provide findings that resemble the results of the "IoTSRM2-based survey study", none and eight of the reviewed related works were found to meet this criterion fully and partially, respectively.

This chapter provided the following contributions:

- The design of a methodology for determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2;
- The design, creation, testing, and distribution of the IoTSRM2-based survey based on the proposed survey methodology;
- The determination of the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2 by analyzing the survey responses and reporting the IoTSRM2-based survey results;
- A comparative analysis of the related work for this IoTSRM2-based survey study based on a proposed set of evaluation criteria.

7. FINAL CONCLUSIONS, CONTRIBUTIONS, AND FUTURE WORK

This chapter provides the final conclusions of this thesis, the thesis contributions, and the future work.

7.1. Final Conclusions

This thesis introduced the doctoral research study, provided overviews of key drivers of and enablers for cybersecurity risk management, critically evaluated the key cybersecurity risk management drivers based on the proposed evaluation methods, provided a critical evaluation of the cybersecurity risk management frameworks based on the proposed evaluation methodology, provided the proposed IoTSRM2, and offered the findings following the IoTSRM2-based survey study.

First, Chapter 1 began with the background of this thesis which is structured in the background of cybersecurity risk management and the background of "Internet of Things (IoT)". With respect to the background of cybersecurity risk management, some of the possible implications for organizations operating in the current digital transformation era from the perspective of cybersecurity were outlined, some of the key cybersecurity risk management concepts were introduced, and then overviews of several renowned cybersecurity risk management standards and methodologies were provided. In terms of the possible implications for organizations embracing technological advances, these include the widening of the attack surface, the incessant evolution of the cyber threat landscape, the ever-growing cybersecurity regulatory ecosystem, and in turn the need to continuously improve the cybersecurity risk management practices in organizations. Furthermore, some of the main cybersecurity risk management concepts relevant for this thesis were defined and outlined, namely some key cybersecurity-related terms, the cybersecurity risk management process, and six cybersecurity domains relevant for cybersecurity risk management strategy. Moreover, an overview of the cybersecurity risk management standards which focuses on two categories of standards (i.e., "cybersecurity risk management", and "generic risk management") was provided. Hence, with respect to the cybersecurity risk management standards, eight standards were outlined that provide requirements for ISMS, general guidelines for ISMS, general guidelines for information security risk management, guidelines on cybersecurity, or requirements for cybersecurity risk management. About the generic risk management standards, three standards were outlined that provide principles and guidelines on risk management or guidelines on risk assessment. Furthermore, Chapter 1 provided an overview of the cybersecurity risk management methodologies which includes a few notable methodologies that match one of the following three categories: "cybersecurity risk assessment", "cybersecurity risk management", and "cybersecurity maturity assessment". Hence, four methodologies were outlined for the cybersecurity risk assessment category, one methodology was described for the cybersecurity risk management category, and one methodology was outlined for the cybersecurity maturity assessment category. Then, with respect the background of "Internet of Things (IoT)", this chapter outlined the various application areas of the IoT, different projections for IoT adoptions highlighting the common consensus for IoT growth, and it introduced some of the key IoT concepts including the components of the "ITU-T's reference model" for IoT. Afterwards, Chapter 1 addressed the motivation, the objectives and structure of this thesis.

Further, Chapter 2 focused on achieving the first four objectives of the thesis, aimed to enable further contributions in the next chapters of the thesis (i.e., Chapters 3-6), and was structured in four parts. The first part of Chapter 2 provided an overview of the cyber threat landscape (i.e., Objectve 1), the second part of Chapter 2 provided an overview of the cybersecurity regulatory landscape (i.e., Objective 2), the third part of Chapter 2 provided an overview of the cybersecurity risk management frameworks (i.e., Objective 3), and the fourth part of Chapter 2 provided an overview of the IoT security best practices (i.e., Objective 4). In the first part of Chapter 2, the overview of the cyber threat landscape was provided by describing thirteen threat categories (i.e., "malware attacks", "social engineering attacks", "denial of service (DoS)", "spam", "insider threat", "hacking attacks", "attacks on privacy and personal data", "cryptojacking", "targeted attacks on critical infrastructure", "supply chain attacks", "cyberpropaganda", and "legal and regulatory sanctions") that resulted following the categorization of the most frequently encountered cybersecurity threats from seventeen relevant and well-renowned sources. In the second part of the chapter, the focus then shifted to provide the overview of cybersecurity regulatory landscape, and Chapter 2 summarized the categories of cybersecurity legislations and regulations that were out of scope and then focused exclusively on the generally applicable laws and regulations pertaining to the selected areas of statute (i.e., "data protection and privacy" and "critical infrastructure protection") from the jurisdictions that exhibited the highest commitment towards cybersecurity worldwide based on the findings from "the Global Cybersecurity Index (GCI)" report (i.e., "European Union", "United States", and "Singapore"). For the European Union, "the General Data Protection Regulation (GDPR)" and "the Directive on Security of Network and Information Systems (NISD)" were outlined. For Singapore, "the Personal Data Protection Act 2012 (PDPA)" and "the Cybersecurity Act (CA)" were covered. As for the United States, at the time of conducting the study on the cybersecurity-related legislations, here was no generally applicable data protection- and privacy-related legislation found at federal level, and "the Critical Infrastructures Protection Act of 2001", "the Executive Order 13636 on Improving Critical Infrastructure Cybersecurity", "the Presidential Policy Directive on Critical Infrastructure Security and Resilience", and "the Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" were identified for the critical infrastructure protection area. It is worth noting that "the NIST's Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)" was identified as being the by-product of the US legislation pertaining to the critical infrastructure protection area.

In the third part of Chapter 2, the definition of cybersecurity risk management frameworks was provided, the frameworks were grouped into three categories (i.e., "cybersecurity-related frameworks", "generic risk management frameworks" and "IT-related frameworks"), and several cybersecurity risk management frameworks that were considered more relevant were described. With respect to "the cybersecurity-related frameworks", ten frameworks were outlined that are applicable to either "risk assessment" or "risk management" activities and are supported by a "risk-based" or "compliance-based" approach. About "the generic risk management frameworks", three frameworks were outlined that provide “generic control objectives”, “internal controls”, “principles”, or “guidelines on risk management”. As for “the IT-related frameworks”, four frameworks were outlined that belong to the following focus areas: “IT service management”, “enterprise IT governance and management”, “enterprise-wide IT risk management”, or “IT capability management”.

In the fourth part of the chapter, Chapter 2 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. Hence, about “the adopter specific IoT security best practices”, Chapter 2 outlined one IoT security framework and three guidelines where each of these guidelines focuses on generic-based IoT security controls, IoT recommendations specific to Identity and Access Management, or healthcare-specific IoT security good practices. With respect to “the general IoT security best practices”, Chapter 2 outlined two codes of practice that focus on secure IoT systems development lifecycle, two guidelines that target sector-specific organizations, one guideline for IoT systems development lifecycle, one guideline for secure IoT supply chain, and three frameworks that address strategic principles or trustworthiness requirements. Regarding “the manufacturer specific IoT security best practices”, Chapter 2 outlined two IoT security standards and four guidelines that give security recommendations, baseline capabilities, or principles for IoT devices. As for “the supplier specific IoT security best practices”, Chapter 2 outlined two codes of practice that provide IoT security measures, two IoT security guidelines, and two IoT security frameworks.

Furthermore, Chapter 3 focused on achieving two objectives of the thesis and was structured in two parts. Therefore, in the first part of Chapter 3, a proposed threat rating method was applied to evaluate the thirteen cyber threat categories (i.e., Objective 5) and in the second part of Chapter 3, the in-scope cybersecurity-related legislations were critically evaluated based on a proposed method (i.e., Objective 6). Thus, the first part of Chapter 3 provided the proposed threat rating method based on a pre-existing taxonomy of organizational cyber harm, a critical evaluation of the cyber threat categories based on the resulted threat ratings, and the related work. First, the proposed threat rating method was outlined. This proposed method allows the analysis of the cyber threat categories, the estimation of the possible extent of applicability to cyber harm of each cyber threat category, and the prioritization of cyber threat categories. Then, the critical evaluation of the selected cyber threat categories was provided and was based on the findings from applying the proposed threat rating method. Hence, three cyber threat categories (i.e., “Targeted attacks on critical infrastructure”, “Malware attacks”, and “Hacking attacks”) resulted in being the most applicable to the types of cyber harm and should be at the top of the list when it comes to cyber threats. Furthermore, seven cyber threat categories (i.e.,“Attacks on privacy and personal data”, “Cyberpropaganda”, “Insider threat”, “Denial of Service (DoS)”, “Supply chain attacks”, “Cyber espionage”, and “Legal and regulatory sanctions”) resulted in having a fairly significant extent of applicability in relation to the whole spectrum of cyber harm and should also be of focal interest for organizations to address cyber threats although these cyber threat categories are not at the top of the list when it comes to cyber threats. Afterwards, one cyber threat category (i.e., “Social engineering attacks”) resulted in having a moderate extent of applicability across all types of cyber harm and should still be seriously addressed by organizations considering that it may be an attack vector for other cyber threats.

Finnaly, two cyber threat categories (i.e., "Cryptojacking" and "Spam") resulted overall as the top least applicable to cyber harm among the thirteen cyber threat categories and should not be overlooked by organizations when it comes to cyber threats as these two threat categories are not negligible. Following the critical evaluation of the thirteen cyber threat categories, Chapter 3 provided the related work in the context of the cyber threat rating methods by discussing the proposed cyber threat rating method in comparison with the threat rating methods. Thus, the proposed cyber threat rating method leveraged the work on cyber harm taxonomy by exploring the potential applicability of the selected thirteen cyber threat categories to the types of cyber harm based on historical data and expert judgement to allow the evaluation of the thirtheen cyber threat categories.

Moreover, the second part of Chapter 3 provided the proposed method for evaluating the in-scope cybersecurity-related legislations, the critical evaluation of these legislations based on the proposed method, and the related work. First, the proposed method was described by introducing, among others, the underlying categories of the "NIST CSF Identify Function" (i.e., "Asset Management", "Business Environment", "Governance", "Risk Assessment", "Risk Management Strategy", "Supply Chain Risk Management"), which were used for comparing the in-scope legislations, and providing the in-scope cybersecurity-related legislations (i.e., "the General Data Protection Regulation – GDPR", "Personal Data Protection Act 2012 – PDPA", "Directive on Security of Network and Information Systems – NISD", "Cybersecurity Act – CA") for the critical evaluation. Further, Chapter 3 outlined the critical evaluation of the selected cybersecurity-related statutes that aimed to identify degree of commonality between the in-scope statutes, and to support organizations in their journey towards achieving regulatory compliance. Thus, the requirements of "GDPR" fairly correspond to three categories (i.e., "Asset Management","Governance", "Supply Chain Risk Management") with minor discrepancies, and partly correspond to three categories (i.e., "Business Environment", "Risk Assessment", "Risk Management Strategy") with some discrepancies. Furthermore, the requirements of "PDPA" partly correspond to the "Governance" category with some discrepancies and nearly deviate from the five categories (i.e., "Asset Management", "Business Environment", "Risk Assessment", "Risk Management Strategy", "Supply Chain Risk Management") of the "NIST CSF Identify Function" with some similarities. Moreover, the requirements of "NISD" fully correspond to two categories (i.e., "Asset Management", "Governance") with no apparent discrepancies and fairly correspond to four categories (i.e., "Business Environment", "Risk Assessment", "Risk Management Strategy", "Supply Chain Risk Management") with minor discrepancies. And, the requirements of "CA" fully correspond to "Asset Management" category with no apparent discrepancies, fairly correspond to the "Risk Assessment" category with minor discrepancies, partly correspond to two categories (i.e., "Business Environment", "Governance") with some discrepancies, and nearly deviate from the two categories (i.e., "Risk Management Strategy", "Supply Chain Risk Management") of the "NIST CSF Identify Function" with some similarities.

Furthermore, Chapter 3 discussed the related work, which revealed that, at the time of conducting the study, much of the literature paid attention to addressing cybersecurity laws in silos, other research works provided an overview of a set of cybersecurity-related laws from a single jurisdiction, other studies investigated only the statutes related to a single cybersecurity area covering multiple jurisdictions and other research works focused on providing cross-references of "GDPR" to different cybersecurity-related frameworks. Thus, no previous research work was found that evaluated all four cybersecurity-related laws (i.e., "GDPR", "NISD", "PDPA", "CA") against the "NIST CSF Identify Function".

Moreover, Chapter 4 focused on achieving Objective 7 of the thesis and provided the proposed methodology for evaluating cybersecurity risk management frameworks, a critical evaluation of selected frameworks, and the related work in the context of cybersecurity risk management frameworks. First, Chapter 4 provided the design of a three-phased methodology that was proposed for evaluating the in-scope cybersecurity risk management frameworks. Here, the three phases of the proposed methodology (i.e., identification of in-scope frameworks, analysis of in-scope frameworks, and comparison of in-scope frameworks) were discussed together with their corresponding inputs and outputs. Furthermore, based on the proposed evaluation methodology, there were eight frameworks identified as in scope: "NIST's Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)", "NIST's Unified Information Security Framework (NIST UISF)", "Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)", "Factor Analysis of Information Risk framework (FAIR)", "Sherwood Applied Business Security Architecture (SABSA)", "MITRE's Cyber Resiliency Engineering Framework (MITRE CREF)", "AICPA's Cybersecurity Risk Management Reporting Framework (AICPA)", and "CIS Controls version 7 framework (CIS)". Then, the critical evaluation of these frameworks was outlined together with the findings which offer a consolidated characterization of the in-scope frameworks and emphasize similarities and differences between them through the thirteen evaluation criteria (i.e., "EC1"-"EC13"). Hence, about the "EC1" (i.e, "Integrated organization-wide risk management") evaluation criterion, this is fully met by the "NIST CSF", "NIST UISF", and "SABSA" frameworks and it is not met by the "OCTAVE", "FAIR", "AICPA", and "CIS" frameworks. About the "EC2" (i.e., "Defines the degree of integration between cybersecurity risk management and operational risk management") evaluation criterion, this is fully met by "NIST CSF", "SABSA", and "CIS" frameworks and it is not met by the remaining frameworks. About the "EC3" (i.e., "Clearly stating guiding principles of the framework") evaluation criterion, this is fully met by the "OCTAVE", "SABSA", "MITRE CREF", "AICPA", and "CIS" frameworks and it is not met by the "FAIR" framework. About the "EC4" (i.e., "Used for undertaking end-to-end cybersecurity risk management rather than developing cybersecurity architectures and solutions") evaluation criterion, this is fully met by the "NIST CSF" and "NIST UISF" frameworks and it applies both ways to the "SABSA" framework. About the "EC5" (i.e., "Relationship to standards or regulatory requirements") and "EC6" (i.e., "Relationship to other frameworks") evaluation criteria, these are fully met by all in-scope cybersecurity risk management frameworks. About the "EC7" (i.e., "Risk-based rather than compliance-based") evaluation criterion, this is fully met by the "NIST CSF", "NIST UISF", "OCTAVE", "FAIR", "SABSA", and "MITRE CREF", it applies both ways to the "CIS" framework, and it is not met by the "AICPA" framework. About the "EC8" (i.e., "Asset-oriented rather than threat-oriented risk analysis approach") evaluation criterion, this is fully met by the "OCTAVE", "FAIR", "SABSA", and "AICPA" frameworks, it applies both ways to the "CIS" framework, and it is not met by the "NIST UISF" framework. About the "EC9" (i.e., "Quantitative rather than qualitative risk assessment approach") evaluation criterion, this is fully met by the "FAIR" framework, it applies both ways to the "SABSA" framework, and it is not met by the "NIST UISF", "OCTAVE", and "CIS" frameworks. About the "EC10" (i.e., "Provides a comprehensive set of recommended cybersecurity controls for managing risk") evaluation criterion, this is fully met by the "NIST UISF", "OCTAVE", "SABSA", "AICPA", and "CIS" frameworks and it is not met by the "FAIR" framework. About the "EC11" (i.e., "Provides guidance relevant to information sharing") evaluation criterion, this is fully met by the "NIST CSF", "NIST UISF", "SABSA", "MITRE CREF", and "AICPA" frameworks and it is not met by the "OCTAVE" and "FAIR" frameworks. About the "EC12" (i.e., "Available supporting documentation – procedures, templates, methods, case studies, etc.") evaluation criterion, this is fully met by the "NIST CSF", "NIST UISF", "OCTAVE", and "CIS" frameworks. As for the "EC13" (i.e., "Periodically updated for continuous improvement") evaluation criterion, this is fully met by all in-scope cybersecurity risk management frameworks, except the "OCTAVE" framework.

Furthermore, the related work in the context of the evaluation of the cybersecurity risk management frameworks was presented in Chapter 4 by looking at the scope of previous research works and by considering the approach adopted by these works to address the scope. With respect to the scope of previous research works, related evaluation studies with a narrower scope and the related evaluation studies with a partly different scope were reviewed. With respect to the approach adopted by related works to address the scope, four types of approach were identified: outlining strenghts and weaknesses, comparison based on the structure of the risk assessment / risk management process, comparison based on defined evaluation criteria, and feature-by-feature comparison. First, the related works about frameworks evaluation with a narrower scope were discussed and classified into two types: research studies with fewer frameworks being addressed and research studies limited to a specific focus area of frameworks. No research was found with fewer frameworks being addressed nor research limited to a specific area of focus was found to provide comparison based on the structure of the risk assessment / risk management process or to provide comparison based on defined evaluation criteria. Also, no research was found to match the type of a narrower scope with fewer frameworks being addressed to provide feature-by-feature comparison. In addition, the following related works with a narrower scope than the critical evaluation provided in Chapter 4 were found and compared with the critical evaluation in question: one research study that outlines the strenghts and weaknesses of fewer frameworks, another research study limited to a specific focus area of frameworks that outlines strenghts and weaknesses, and three research works limited to a specific focus area of frameworks that provide a feature-by-feature comparison. Second, the related evaluation studies with a partly different scope were discussed and classified into two types: research studies addressing best-practices irrespective of types and research studies merely-focusing on the risk assessment / risk management related methodologies/methods. With respect to the research studies addressing best-practices irrespective of types, the following related works were found and compared with the critical evaluation in question: one research study outlining stregths and weaknesses, one research study providing comparison based on the structure of the risk assessment / risk management process, another research study providing comparison based on defined evaluation criteria, and two research studies providing feature-by-feature comparison. With respect to the research studies merely-focusing on the risk assessment / risk management related methodologies/methods, the following related works were found and compared with the critical evaluation in question: one research study outlining stregths and weaknesses, two research studies providing comparison based on the structure of the risk assessment/ risk management process, four research studies providing comparison based on defined evaluation criteria, and three research studies providing feature-by-feature comparison.

Moreover, Chapter 5 focused on achieving Objective 8 of the thesis and provided the proposed methodology for developing the IoT security risk management strategy reference model, the proposed "IoT security risk management strategy reference model (IoTSRM2)", the evaluation of selected informative references of "IoTSRM2", and the comprehensive analysis of the related work for "IoTSRM2". First, the three-phased methodology for developing the "IoTSRM2" was described and consisted of nine steps and outputs, namely three steps with associated outputs for each of the three phases (i.e., "Scoping", "Analysis", and "Creation").

Afterwards, the proposed "IoTSRM2" was described as part of Chapter 5. The proposed "IoTSRM2" consists of 6 domains, 16 objectives, and 30 controls for IoT adopters from any sector, which should be addressed by both IoT adopters and IoT suppliers. First, an illustrative overview of the proposed "IoTSRM2" was provided. Then, for each informative reference of the proposed "IoTSRM2", the total number of unique in-scope IoT security requirements mapped to the "IoTSRM2" controls was provided. Next, the "IoTSRM2" objectives were provided for each "IoTSRM2" domain, the "IoTSRM2" controls were described in line with the target information granularity for each "IoTSRM2" objective, and, among others, the prioritization of "IoTSRM2" controls based on their adjusted weights was provided.

Moreover, the critical evaluation of selected informative references of "IoTSRM2" based on their percentage-wise linkage to "IoTSRM2" from Chapter 5 included the overall evaluation of selected informative references and individual evaluations of selected informative references for each "IoTSRM2" domain. With respect to the overall evaluation of selected seven informative references (i.e., Refs. [Age20a], [CSA19a], [ENI18b], [ENI20a], [IoT16], [IoT20a], and [NIS20a]), it outlined the critical evaluation of the selected informative references relative to their percentage-wise linkage to the "IoTSRM2" domains and to the entire "IoTSRM2", and the critical evaluation of the selected informative references based on their number of in-scope IoT security requirements for each "IoTSRM2" domain. With respect to the percentage-wise linkage of the selected informative references to each "IoTSRM2" domain, Refs. [Age20a], [CSA19a], [ENI18b], and [IoT20a] each resulted as the most linked to some of the "IoTSRM2" domains. In addition, with respect to the percentage-wise linkage of the selected informative references to the entire "IoTSRM2", Refs. [ENI18b], [CSA19a], and [Age20a] resulted in being the top three most linked to "IoTSRM2", in that order. In addition, Refs. [Age20a], [ENI18b], [IoT20a] and [NIS20a] resulted in being the most focused on the "Governance" domain. Then, with respect to the individual evaluations of selected informative references for each "IoTSRM2" domain, the selected informative references were critically evaluated relative to their percentage-wise linkage to the objectives of the "IoTSRM2" domain and to the entire "IoTSRM2" domain. Firstly, the findings revealed that Refs. [CSA19a], [ENI18b], and [NIS20a] are the top three most linked to the "Asset Management" domain, in that order. Secondly, the findings revealed that Refs. [ENI18b], [Age20a], and [ENI20a] are the top three most linked to "Business Environment" domain, in that order, where both Refs. [Age20a] and [ENI20a] share the same position. Thirdly, the findings revealed that Refs. [ENI18b], [IoT20a], and [CSA19a] are the top three most linked to the "Governance" domain, in that order. Fourthly, the findings revealed that Refs. [CSA19a], [ENI18b], and [IoT16] are the top three most linked to "Risk Assessment" domain, in that order. Fifthly, the findings revealed that Refs. [CSA19a], [ENI18b], and [IoT20a] are the top three most linked to "Risk Management Strategy" domain, where they all share the same position. Sixthly and finally, the findings revealed that Refs. [Age20a], [ENI18b], and [CSA19a] are the top three most linked to "Supply Chain Risk Management" domain, in that order.

Furthermore, the comprehensive analysis of the related work for "IoTSRM2" was presented in Chapter 5 through the comparison of the proposed "IoTSRM2" with the 25 selected IoT security best practices based on eight evaluation criteria and three types of applicability to each evaluation criterion (i.e., "E1"-"E8"). Hence, about the "E1" (i.e., "Focus on strategic IoT security practices over technical IoT security practices") evaluation criterion, this fully applies to seven informative references and the "IoTSRM2" and applies to a certain extent, but not fully, to ten informative references. About the "E2" (i.e., "Methodology for developing the recommended IoT security requirements / controls is clearly described") evaluation criterion, this fully applies to seven informative references and the "IoTSRM2" and applies to a certain extent, but not fully, to four informative references. About the "E3" (i.e., "Mapping of IoT security requirements / controls to NIST CSF's Categories and Subcategories") evaluation criterion, this fully applies to the "IoTSRM2" and applies to a certain extent, but not fully, to two informative references. About the "E4" (i.e., "Clearly indicate for each IoT security requirement / control expected IoT security actions / activities from IoT suppliers of the target audience") evaluation criterion, this fully applies to the "IoTSRM2" and applies to a certain extent, but not fully, to ten informative references. About the "E5" (i.e., "Provides integration points with the cybersecurity program as part of each IoT security requirement / control") evaluation criterion, this fully applies to the "IoTSRM2" and applies to a certain extent, but not fully, to four informative references. About the "E6" (i.e., "Mapping of relevant IoT security best practices with unique identifiers to each recommended IoT security requirement / control") evaluation criterion, this fully applies to two informative references and the "IoTSRM2" and applies to a certain extent, but not fully, to eleven informative references. About the "E7" (i.e., "Prioritization of the recommended IoT security requirements / controls") evaluation criterion, this fully applies to three informative references and the "IoTSRM2" and applies to a certain extent, but not fully, to four informative references. Finally, about the "E8" (i.e., "Provides statistics for the mapping of informative references") evaluation criterion, this fully applies to one informative reference and the "IoTSRM2" and it does not apply to the remaining informative references.

Furthermore, Chapter 6 focused on achieving Objective 9 of the thesis. It provided the 14 research questions for the "IoTSRM2-based survey study", the proposed survey methodology for addressing the research questions, the survey results following the analysis of the survey responses of leaders from industries and governments from around the world, and the comprehensive analysis of the related work for the "IoTSRM2-based survey study" using seven evaluation criteria. Following the introduction of the 14 research questions for the "IoTSRM2-based survey study", the three-phased survey methodology for addressing the 14 research questions was described and consisted of nine steps and outputs, namely three steps with associated outputs for each of the three phases (i.e., the "Plan and Create", "Launch and Run", and "Analyze and Report" phases). Subsequently, Chapter 6 presented the survey results for three groups of surveyed organizations (i.e., "the surveyed large and small-medium organizations", "the surveyed large organizations", "the surveyed large TMT organizations"). Hence, with respect to the results for "the surveyed large and small-medium organizations", these results revealed that the "C-level executive and/or board member" and "Consulting practice leader and/or principal" position levels are the top position levels of the survey respondents for the surveyed organizations, the "Large Organization" category is the top organization type for these organizations, the "Technology, Media, & Telecom (TMT)" industry sector is the top industry sector for the surveyed organizations, and that "North/South America" region is the top region for the surveyed organizations. Furthermore, about the overall tendency of the IoT security risk management strategies of the surveyed organizations relative to the "IoTSRM2" controls, the findings suggested, among others, that the majority of organizations engage in IoT risk assessments, focus on improving the resilience of their IoT infrastructures, lack all-encompassing IoT asset inventories, adopt either one-size-fits-all or ad hoc IoT security risk management approaches, underperform when it comes to IoT supply chain risk management, and underperform in strategizing IoT governance and risk management.Then, about "the overall average IoTSRM2 compliance score" of the surveyed organizations for each "IoTSRM2" control, the majority of the surveyed organizations appeared to do better when it comes to the "Resiliency requirements", "IoT security operations roles and responsibilities", and "IoT risk identification and analysis" controls of the "IoTSRM2", and these surveyed organizations should consider fast-tracking the improvement of their capabilities related to the "IoT security training and awareness plan", "IoT supplier contract management plan", "IoT End-of-Life plan", "IoT software assets inventory", "IoT supply chain risk assessment", and "Criticality and impact analysis" controls of the "IoTSRM2" where they appeared to underperform. As for "the IoTSRM2 compliance score" of each of the surveyed organizations, the results revealed, among others, that the top three highest and lowest "IoTSRM2 compliance scores" for the surveyed organizations correspond to large (i.e., except for one of them) and small-medium organizations, respectively.

Furthermore, with respect to the results for "the surveyed large organizations", these results revealed that the "Consulting practice leader and/or principal" position levels is the top position level of the survey respondents for the surveyed large organizations, the "Technology, Media, & Telecom (TMT)" industry sector is the top industry sector for the surveyed large organizations, and that the "North/South America" region is the top region for the surveyed large organizations. In addition, with respect to "the overall average IoTSRM2 compliance score" of the surveyed large organizations for each "IoTSRM2" control, the majority of the surveyed large organizations appeared to perform better in terms of the "Resiliency requirements", "IoT security operations roles and responsibilities", "Cybersecurity regulatory framework" and "IoT security policy" controls of the "IoTSRM2", and these surveyed large organizations should consider accelerating the improvement of their capabilities related to the "IoT software assets inventory", "IoT hardware assets inventory", "IoT End-of-Life plan", "End-of-Life policy" and "Criticality and impact analysis" controls of the "IoTSRM2".

Moreover, with respect to the results for "the surveyed large TMT organizations", the results revealed that the "Consulting practice leader and/or principal" and "C-level executive and/or board member" position levels are the top position levels of the survey respondents for the surveyed large TMT organizations and that the "North/South America" region is the top region for the surveyed large TMT organizations. In addition, with respect to "the overall average IoTSRM2 compliance score" of the surveyed large TMT organizations for each "IoTSRM2" control, the majority of the surveyed large TMT organizations appeared to perform better when it comes to the "IoT security policy", "Disclosure-based IoT vulnerability discovery", "IoT risk identification and analysis", "IoT vulnerability management plan", "Assessment-based IoT vulnerability discovery", "Context-informed IoT security risk tolerances", "IoT trustworthiness requirements", "Cybersecurity risk register and IoT risk responses", "IoT supply chain risk management plan", and "IoT supplier contract management plan" controls of the "IoTSRM2", and these surveyed large TMT organizations should consider boosting the pace of the improvement of their capabilities related to the "Criticality and impact analysis", "Vulnerability disclosure policy", "IoT software assets inventory", and "IoT security training and awareness plan" controls of the "IoTSRM2".

Further, Chapter 6 discussed the "IoTSRM2-based survey study" in relation to the selected related studies using seven evaluation criteria based on the proposed methodology and using three types of applicability to each evaluation criterion (i.e., "the evaluation criterion fully applies", "the evaluation criterion applies to a certain Extent", and "the as-is evaluation criterion does not apply"). Hence, about the "E1" (i.e., "The research study is focused on determining the current state of IoT security risk management strategies in organizations") evaluation criterion, this fully applies to the "IoTSRM2-based survey study" and applies to a certain extent to 12 related studies. About the "E2" (i.e., "The methodology for achieving the intended purpose of the research study is clearly described") evaluation criterion, this fully applies to one related study and the "IoTSRM2-based survey study" and applies to a certain extent to five related studies. About the "E3" (i.e., "The underlying design best practice of the research method of the methodology, is clearly documented") evaluation criterion, this fully applies to the "IoTSRM2-based survey study" and applies to a certain extent to one related study. About the "E4" (i.e., "Provides results for organizations of a specific organization size") evaluation criterion, this fully applies to three related studies and the "IoTSRM2-based survey study" and does not apply to the other related studies. About the "E5" (i.e., "Provides results for organizations from a specific industry sector") evaluation criterion, this fully applies to four related studies and the "IoTSRM2-based survey study" and does not apply to the other related studies. About the "E6" (i.e., "The results reveal the level of compliance of each subject with a reference model") evaluation criterion, this fully applies to the "IoTSRM2-based survey study" and applies to a certain extent to one related study. Finally, about the "E7" (i.e., "The findings resemble the results of the IoTSRM2-based survey") evaluation criterion, this fully applies to the "IoTSRM2-based survey study" and applies to a certain extent to eight related studies.

7.2. Thesis Contributions

Each chapter of this doctoral thesis provided the corresponding contributions of the author. These contributions are outlined in Tables 7.1, 7.2, and 7.3.

Table 7.1. Theoretical contributions

No.	Contribution	Chapter No.	Reference[1]
1.	The definition of the „standard", „method", and „methodology" terms to clearly delineate the distinction between them	1	[Giu+21]
2.	The definition of the „cybersecurity risk management framework" term to enable a common understanding of this term	2	[Giu+21]
3.	The development of a novel taxonomic hierarchy that classifies IoT security best practices based on their applicability to specific groups of target audience and type of IoT security best practice	2	[Pop+21a]
4.	A comparison of the proposed threat rating method with the related work	3	[Pop+19b]

No.	Contribution	Chapter No.	Reference[1]
5.	An analysis of the related work relevant to the evaluation of cybersecurity-related legislations	3	[Pop+19a]
6.	A comprehensive analysis of the related work relevant to the evaluation of cybersecurity risk management frameworks that delved into previous studies with a narrower scope and a partly different scope	4	[Pop20]
7.	A comparative analysis of the related work for the proposed reference model based on a proposed set of evaluation criteria	5	[Pop+21a]
8.	A comparative analysis of the related work for this IoTSRM2-based survey study based on a proposed set of evaluation criteria	6	[Pop+21b]

[1] Note that these references indicate publications and/or scientific reports of the author of this thesis.

Table 7.2. Theoretical contributions applicable in practice

No.	Contribution	Chapter No.	Reference[1]
1.	The identification, categorization, and description of standards and methodologies relevant to cybersecurity risk management based on the study of the literature on cybersecurity risk management	1	[Giu+21]
2.	The determination and categorization of current cyber threats into thirteen up-to-date cyber threat categories along with the description of these cyber threat categories based on the investigation of seventeen relevant and well-renowned sources	2	[Pop+19b]
3.	An overview of the cybersecurity-related legislations and regulations pertaining to two cybersecurity areas of statute for three separate jurisdictions	2	[Pop+19a]
4.	The identification, categorization, and description of frameworks relevant to cybersecurity risk management based on the study of the literature on the cybersecurity risk management	2	[Giu+21]
5.	The identification, classification, and description of IoT security best practices based on the study of literature and the proposed taxonomic hierarchy	2	[Pop+21a]
6.	The design of a novel cyber threat rating method and the creation of a threat rating tool	3	[Pop+19b]
7.	The design of a new method for evaluating selected key cybersecurity-related legislations	3	[Pop+19a]
8.	The design of a three-phased methodology that involves identification, analysis, and comparison of in-scope cybersecurity risk management frameworks	4	[Pop20]

No.	Contribution	Chapter No.	Reference[1]
9.	The development of a hierarchical structure for evaluating the in-scope cybersecurity risk management frameworks, which includes seven dimensions and thirteen evaluation criteria	4	[Giu+21]
10.	The definition of six linguistic values for rating the in-scope cybersecurity risk management frameworks against the evaluation criteria	4	[Giu+21]
11.	The design of a methodology for developing the IoT security risk management strategy reference model based on best practices	5	[Pop+21a]
12.	The design of a methodology for determining the current state of IoT security risk management strategies in the surveyed organizations relative to the IoTSRM2	6	[Pop+21b]

[1] Note that these references indicate publications and/or scientific reports of the author of this thesis.

Table 7.3. Practical contributions

No.	Contribution	Chapter No.	Reference[1]
1.	The application of the proposed cyber threat rating method to thirteen cyber threat categories for evaluating these cyber threat categories	3	[Pop+19b]
2.	The critical evaluation of the thirteen cyber threat categories based on their possible extents of applicability to cyber harm	3	[Pop+19b]
3.	The critical evaluation of the in-scope cybersecurity-related legislations to establish the degree of commonality between them from the perspective of organizational understanding to managing cybersecurity risk	3	[Pop+19a]
4.	The critical evaluation of eight cybersecurity risk management frameworks based on the proposed evaluation methodology	4	[Giu+21]
5.	The development of a reference model for IoT security risk management strategy that is suitable for IoT adopters from any sector based on the proposed methodology	5	[Pop+21a]
6.	A critical evaluation of selected informative references of the IoTSRM2 based on their linkage to the proposed reference model	5	[Pop+21a]
7.	The design, creation, testing, and distribution of the IoTSRM2-based survey based on the proposed survey methodology	6	[Pop+21b]
8.	The determination of the current state of IoT security risk management strategies in the surveyed organizations	6	[Pop+21b]

No.	Contribution	Chapter No.	Reference[1]
	relative to the IoTSRM2 by analyzing the survey responses and reporting the IoTSRM2-based survey results		

[1] Note that these references indicate publications and/or scientific reports of the author of this thesis.

This thesis is supported by five research papers. The list of the publications was tagged according to the type of the publication: ISI Journal, ISI Conference Proceedings and Springer Book Chapter. Thus, the list of the publications is the following:

- **Popescu, T.M.**, Popescu, A.M., & Prostean, G. (2021a). IoT Security Risk Management Strategy Reference Model (IoTSRM2). *Future Internet*, *13* (6), 148. https://doi.org/10.3390/fi13060148 **(ISI Journal)**
- **Popescu, T.M.**, Popescu, A.M., & Prostean, G. (2021b). Leaders' Perspectives on IoT Security Risk Management Strategies in Surveyed Organizations Relative to IoTSRM2. *Applied Sciences, 11* (19), 9206. https://doi.org/10.3390/app11199206 **(ISI Journal)**
- Giuca, O., **Popescu, T.M**., Popescu, A.M., Prostean, G., & Popescu, D.E. (2021). A Survey of Cybersecurity Risk Management Frameworks. In V. Balas, L. Jain, M. Balas & S. Shahbazova (Eds.), *Soft Computing Applications. SOFA 2018. Advances in Intelligent Systems and Computing* (Vol. 1221, pp. 240-272). Cham: Springer. https://doi.org/10.1007/978-3-030-51992-6_20 **(Springer Book Chapter)**
- **Popescu, T.M.**, Popescu, A.M., Prostean, G., & Popescu, D.E. (2019a). Evaluation of legislations from the perspective of organizational understanding to managing cybersecurity risk. In K.S. Soliman (Eds.) *Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020* (pp. 4677-4689). ISBN: 978-0-9998551-2-6 **(ISI Conference Proceedings)**
- **Popescu, T.M.**, Popescu, A.M., Prostean, G., & Popescu, D.E. (2019b). Cybersecurity Threat Rating Method Based on Potential Cyber Harm', In: Soliman K. S. (Eds.) *Proceedings of the 34th International Business Information Management Association Conference (IBIMA). Vision 2025: Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage* (pp. 5909- 5920). ISBN: 978-0-9998551-3-3 **(ISI Conference Proceedings)**

The PhD reports that were presented are the following:

- **Popescu, T.M.** (2020). *Cybersecurity Risk Management* (Ph.D. Report 1). Politehnica University of Timisoara, Timisoara, Romania.
- **Popescu, T.M.** (2021). *IoT Security Risk Management Strategy* (Ph.D. Report 2). Politehnica University of Timisoara, Timisoara, Romania.

7.3. Future Work

Throughout this research work, several possible future research directions were identified on the cybersecurity risk management drivers and enablers.

Firstly, with respect to the research work on the cyber threat landscape, future work may include redoing the overview of the cyber threat landscape after a certain time in order to ensure that the thirteen cyber threat categories remain relevant and up to date. In addition, after reconducting this study on the cyber threat categories, future work may involve rating the resulted cyber threat categories using the proposed cyber threat rating method of this thesis along with a comparative analysis of the findings from this thesis with the ones from this future work.

Secondly, with respect to research work on the cybersecurity regulatory landscape, future work may involve extending the overview of the cybersecurity-related legislations and regulations after a certain time to include more areas of statute (e.g., IoT security laws) and more jurisdictions or the jurisdictions that will show the greatest level of commitment towards cybersecurity when this study will be conducted. In addition, after performing this study, another future work may involve an extension of the critical evaluation of the cybersecurity-related legislations and regulations from this thesis by analyzing the legal requirements against the Categories of all Functions of the "NIST Cybersecurity Framework".

Thirdly, with respect to research work on the cybersecurity risk management frameworks, future work may involve extending the critical evaluation to include framework enablers (e.g., standards, methodologies).

Fourthly, with respect to research work on the proposed "IoTSRM2", future work may include several projects such as the implementation of the "IoTSRM2" in organizations, the extension of the "IoTSRM2" to include all Functions of the "NIST Cybersecurity Framework", and the undertaking of a survey based on the extended version of the "IoTSRM2".

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

APPENDICES

A1. List of Publications

ISI Journals:

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

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

ISI Conference Proceedings:

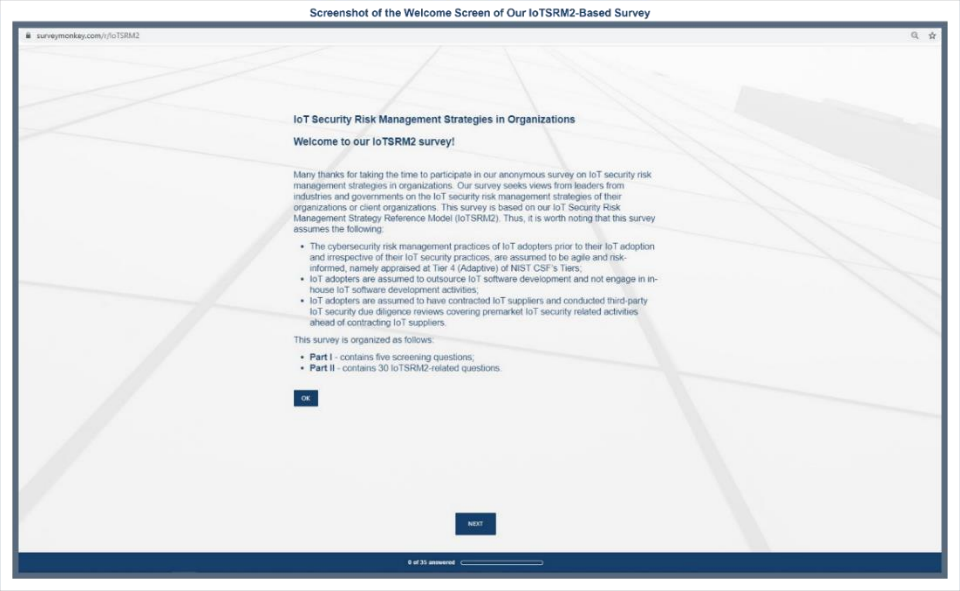
1. **Popescu, T.M.**, Popescu, A.M., Prostean, G., & Popescu, D.E. (2019). Evaluation of legislations from the perspective of organizational understanding to managing cybersecurity risk. In K.S. Soliman (Eds.) *Proceedings of the 33rd International Business Information Management Association Conference,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

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

Book Chapter:

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

A2. Selected Screenshots from the IoTSRM2-Based Survey



Screenshot of the Welcome Screen of Our IoTSRM2-Based Survey

IoT Security Risk Management Strategies in Organizations

Welcome to our IoTSRM2 survey!

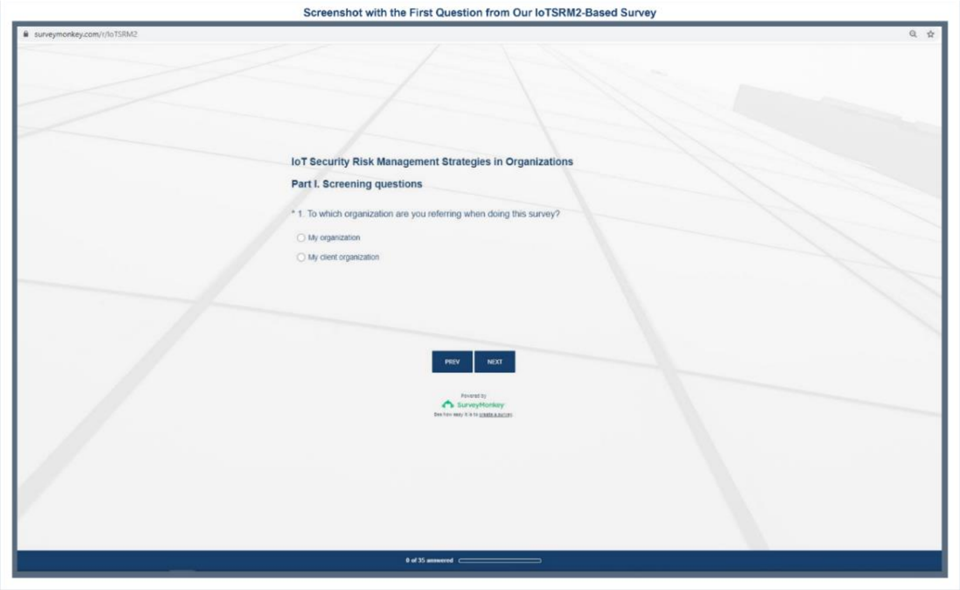
Many thanks for taking the time to participate in our anonymous survey on IoT security risk management strategies in organizations. Our survey seeks views from leaders from industries and governments on the IoT security risk management strategies of their organizations or client organizations. This survey is based on our IoT Security Risk Management Strategy Reference Model (IoTSRM2). Thus, it is worth noting that this survey assumes the following:

- 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;
- 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.

This survey is organized as follows:

- **Part I** - contains five screening questions;
- **Part II** - contains 30 IoTSRM2-related questions.

Fig. A2.1. Screenshot of the welcome screen of the IoTSRM2-based survey [Pop+21b]



Screenshot with the First Question from Our IoTSRM2-Based Survey

surveymonkey.com/r/IoTSRM2

IoT Security Risk Management Strategies in Organizations

Part I. Screening questions

* 1. To which organization are you referring when doing this survey?

○ My organization

○ My client organization

PREV
NEXT
Powered by
SurveyMonkey
See how easy it is to create a survey.
0 of 35 answered

Fig. A2.2. Screenshot with the first question from the IoTSRM2-based survey [Pop+21b]

A3. Summary of the IoTSRM2-Based Survey Responses in Numbers

Table A3.1. Summary of the survey responses in numbers per IoTSRM2 controls and related questions [Pop+21b]

IoTSRM2 Question ID	**IoTSRM2 Control**	**No. of “No, to a great extent”**	**No. of “No, to a certain extent”**	**No. of “Yes, to a certain extent”**	**No. of “Yes, to a great extent”**
“6”	“IoT hardware assets inventory”	“6”	“12”	“10”	“3”
“7”	“IoT software assets inventory”	“8”	“11”	“11”	“1”
“8”	“Criticality and impact analysis”	“5”	“12”	“13”	“1”
“9”	“Resiliency requirements”	“5”	“5”	“15”	“6”
“10”	“IoT security policy”	“5”	“9”	“13”	“4”
“11”	“Privacy policy”	“7”	“7”	“16”	“1”
“12”	“Vulnerability disclosure policy”	“7”	“9”	“12”	“3”
“13”	“End-of-Life policy”	“7”	“12”	“11”	“1”
“14”	“IoT security governance structures and responsibilities”	“5”	“9”	“12”	“5”
“15”	“IoT security operations roles and responsibilities”	“5”	“6”	“14”	“6”
“16”	“Cybersecurity regulatory framework”	“6”	“7”	“13”	“5’
“17”	“IoT security and privacy controls management plan”	“5”	“11”	“12”	“3”
“18”	“IoT security budget plan”	“6”	“10”	“11”	“4”
“19”	“IoT security measurement and reporting plan”	“8”	“10”	“11”	“2”

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

BIBLIOGRAPHY

[Acc18] Accenture. (2018). *Cyber Threatscape Report 2018 Midyear Cybersecurity Risk Review*. Accenture. Retrieved August 7, 2019, from https://www.accenture.com/t20180803t064557z__w__/us-en/_acnmedia/pdf-83/accenture-cyber-threatscape-report-2018.pdf

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

[Age20b] AgeLight LLC. (2020b). *IoT Safety & Trust Design Architecture and Risk Assessment Toolkit*. AgeLight LLC. Retrieved February 23, 2021, from https://www.agelight.com/iot

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

[AIC17a] AICPA. (2017a). *SOC 2® examinations and SOC for Cybersecurity examinations: Understanding the key distinctions*. Association of International Certified Professional Accountants. Retrieved January 10, 2019, from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/soc-2-vs-cyber-whitepaper-web-final.pdf

[AIC17b] AICPA. (2017b). *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Association of International Certified Professional Accountants. Retrieved January 10, 2019, from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

[AIO16] AIOTI. (2016). *Report on Workshop on Security and Privacy in the Hyper-Connected World*. Alliance for Internet of Things Innovation. Retrieved July 22, 2020, from https://aioti.eu/aioti-wg03-reports-on-iot-standards/

[Alb+01] Alberts, J.C., & Dorofee, A.J. (2001). *OCTAVE Criteria, Version 2.0* (CMU/SEI-2001-TR-016). Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pa. Retrieved January 10, 2019, from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2001_005_001_13871.pdf

[Ali+14] Ali, S., Padmanabhan, V., & Dixon, J. (2014). *Why Cybersecurity is a Strategic Issue*. Bain & Company, Inc. Retrieved January 10, 2019, from https://www.bain.com/insights/why-cybersecurity-is-a-strategic-issue/

[Alm+17] Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT), 7* (3), 51–62. https://doi.org/10.5121/csit.2017.70305

[Alm+21] Almutairi, O., & Almarhabi, K. (2021). Investigation of Smart Home Security and Privacy: Consumer Perception in Saudi Arabia. *International Journal of Advanced Computer Science and Applications (IJACSA), 12*. http://dx.doi.org/10.14569/IJACSA.2021.0120477

[Als+19] Alshohoumi, F.K., Sarrab, M., AlHamadani, A., & Al-Abri, D. (2019). Systematic review of existing IoT architectures security and privacy issues and concerns. *International Journal of Advanced Computer Science and Applications*, *10* (7), 232-251. https://doi.org/10.14569/ijacsa.2019.0100733

[Arm21] Arm Limited. (2021). *Bridging the Gap PSA Certified Security Report 2021 How collaboration will secure the future of IoT*. Arm Limited. Retrieved June 7, 2021, from https://report.psacertified.org/

[Asp+16] Asplund, M., & Nadjm-Tehrani, S. (2016). Attitudes and Perceptions of IoT Security in Critical Societal Services. *IEEE Access, 4*, 2130-2138. https://doi.org/10.1109/ACCESS.2016.2560919

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

[ATK19] A.T. Kearney. (2019). *Maintaining the Human Connection in an Age of AI 2019 Views from the C-Suite An Annual Survey of Global Business Executives*. A.T. Kearney, Inc. Retrieved April 2, 2021, from https://www.kearney.com/web/global-business-policy-council/views-from-the-c-suite

[AT&T16] AT&T. (2016). *AT&T Cybersecurity Insights: The CEO's Guide to Securing the Internet of Things*. AT&T. Retrieved March 19, 2021, from https://www.business.att.com/content/dam/attbusiness/insights/migrated/exploring iotsecurity.pdf

[Aus17] Australian Government. (2017). *What is the Critical Infrastructure Centre?* Australian Government. Retrieved February 03, 2019, from https://cicentre.gov.au/resources

[Avi+02] Avison, D., & Fitzgerald, G. (2002). *Information Systems Development – Methodologies, Techniques and Tools.* (3rd ed). UK: McGraw-Hill Education.

[Axe12] Axelos. (2012). *MoR Glossary of Terms – English*. AXELOS Limited. Retrieved January 10, 2019, from https://www.axelos.com/Corporate/media/Files/Glossaries/MoR-Glossary-of-Terms_GB.pdf

[Bai18] Bain & Company. (2018). *Cybersecurity Is the Key to Unlocking Demand in the Internet of Things*. Bain & Company. Retrieved April 4, 2021, from https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things/

[Ban16] Bank of England. (2016). *CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations*. London: Bank of England

[Bel+11] Belk, M., Coles, M., Goldschmidt, C., et al. (2011). *Fundamental Practices for Secure Software Development 2ND EDITION A Guide to the Most Effective Secure Development Practices in Use Today*. Software Assurance Forum for Excellence in Code (SAFECode). Retrieved March 19, 2021, from http://safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf

[BIT16] BITAG. (2016). *Internet of Things (IoT) Security and Privacy Recommendations*. Broadband Internet Technical Advisory Group. Retrieved July 22, 2020, from https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[Bod+11] Bodeau, D.J., & Graubart, R. (2011). *Cyber Resiliency Engineering Framework* (MTR110237). The MITRE Corporation. Retrieved January 10, 2019, from https://www.mitre.org/sites/default/files/pdf/11_4436.pdf

[Boo19] Booz Allen Hamilton. (2019). *2019 Cyber Threat Outlook Eight ways threat actors will make waves in 2019*. Booz Allen Hamilton. Retrieved August 7, 2019, from https://www.boozallen.com/c/insight/publication/top-8-cybersecurity-trends-for-2019.html

[Bra+19] Brass, I., Pothong, K., & Haitham, M. (2019). *Navigating and Informing the IoT Standards Landscape: A Guide for SMEs and Start-Ups*. BSI, PETRAS IoT.

[BSI08a] BSI. (2008a). *BSI-Standard 100-1: Information Security Management Systems (ISMS) Version 1.5*. Federal Office for Information Security. Retrieved January 10, 2019, from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1

[BSI08b] BSI. (2008b). *BSI-Standard 100-2: IT-Grundschutz Methodology Version 2.0*. Federal Office for Information Security. Retrieved January 10, 2019, from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile

[BSI17] BSI Group. (2017). *Emerging trends in the cyber landscape – 2018*. The British Standards Institution. Retrieved January 10, 2019, from https://www.bsigroup.com/contentassets/d6a55cdd1c7f4849811d48e6397340b7/csir---emerging_cyber_trends.pdf?amp;epslanguage=fr-FR

[BSI18] BSI Group. (2018). *What is a standard? & What does it do?* The British Standards Institution. Retrieved January 10, 2019, from https://www.bsigroup.com/en-GB/standards/Information-about-standards/what-is-a-standard/

[Cab11a] Cabinet Office. (2011a). *The UK cyber security strategy: protecting and promoting the UK in a digital world*. London: Crown

[Cab11b] Cabinet Office and HMG. (2011b). *HMG IA Standard No. 6 Protecting Personal Data and Managing Information Risk*. Crown. Retrieved January 10, 2019, from https://data.gov.uk/data/contracts-finder-archive/download/611325/439bbc8a-9249-4210-93a8-8c33edcba603

[Cab20] Cabinet Office. (2020). *Consumer Attitudes Towards IoT Security*. Cabinet Office. Retrieved June 7, 2021, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978685/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf (accessed on 7 June 2021).

[Cam19] Cambridge University Press. (2019). *Cambridge Dictionary*. Cambridge University Press. Retrieved September 8, 2019, from https://dictionary.cambridge.org/dictionary/english/harm

[Car+17] Carrapico, H., & Barrinha, A. (2017). The EU as coherent (cyber) security actor? *Journal of Common Market Studies*, 55 (6), 1254–1272.

[Car+18] Carrapico, H., & Barrinha, A. (2018). European Union cyber security as an emerging research and policy field. *European Politics and Society*, *19* (3), 299-303.

[Car16] Carnegie Mellon University. (2016). *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide*. Carnegie Mellon University. Retrieved January 10, 2019, from https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-method-description-and-user-guide.pdf

[Car16a] Carr, M. (2016a). Crossed Wires: International Cooperation on Cyber Security. *Interstate-Journal of International Affairs*, *2015* (2), 1-10.

[Ceb+14] Cebula, J.J., Popeck, M.E., & Young, L.R. (2014). *A Taxonomy of Operational Cyber Security Risks Version 2* (CMU/SEI-2014-TN-006). Software Engineering Institute. Retrieved August 8, 2019, from http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=91013

[Cha+15] Chaudhary, R., & Hamilton, J. (2015). *The Five Critical Attributes of Effective Cybersecurity Risk Management*. Crowe Horwath. Retrieved January 10, 2019, from https://www.crowe.com/insights/asset/t/the-five-critical-attributes-of-effective-cybersecurity-risk-managemen

[Chm+14] Chmielecki, T., Chołda, P., Pacyna, P., Potrawka, P., Rapacz, N., Stankiewicz, R., & Wydrych, P. (2014). Enterprise-oriented Cybersecurity Management. In M. Ganzha, L. Maciaszek, & M. Paprzycki (Eds.), *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems* (pp. 863-

870). Annals of Computer Science and Information Systems (ACSIS), 2. http://dx.doi.org/10.15439/2014F38

[Cis17] Cisco. (2017). *Cybersecurity Management Program*. Cisco. Retrieved January 10, 2019, from https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-management-programs.pdf

[CIS18a] CIS. (2018a). *Top 10 Malware January 2018*. Center for Internet Security. Retrieved January 10, 2019, from https://www.cisecurity.org/top-10-malware-january-2018/

[CIS18b] CIS. (2018b). *CIS RAM Version 1.0 Center for Internet Security Risk Assessment Method For Reasonable Implementation and Evaluation of CIS Controls TM*. Center for Internet Security. Retrieved January 10, 2019, from https://learn.cisecurity.org/cis-ram

[CIS18c] CIS. (2018c). *CIS Controls Framework*. Center for Internet Security. Retrieved January 10, 2019, from https://www.cisecurity.org/controls/

[CMS18] CMS Cameron McKenna Nabarro Olswang. (2018). *A guide to GDPR for companies in Singapore*. CMS Cameron McKenna Nabarro Olswang LLP. Retrieved February 12, 2019, from https://cms.law/en/content/download/355105

[CNS15] CNSSI. (2015). *Committee on National Security Systems (CNSS) Glossary*. National Security Agency, Fort Meade

[Cob+18] Coburn, A., et al. (2018). *Cyber Risk Outlook*. Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc.

[Com+10] Combs, J.P., & Onwuegbuzie, A.J. (2010). Describing and illustrating data analysis in mixed research. *International Journal of Education, 2*, 1-23. https://doi.org/10.5296/ije.v2i2.526

[Com05] Commission of the European Communities. (2005). *Green Paper on a European Programme for Critical Infrastructure Protection*. Brussels: Official Journal of the European Union. Retrieved February 03, 2019, from https://eur-lex.europa.eu/

[Com20] Commonwealth of Australia. (2020). *Code of Practice Securing the Internet of Things for Consumers*. Australian Government. Retrieved January 07, 2021, from https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

[Con19] Concurrency. (2019). *Concurrency NIST Framework Map to Microsoft Technologies*. Concurrency, Inc. Retrieved February 12, 2019, from https://www.concurrency.com/landing/nist

[Cop20] Copper Horse. (2020). *Mapping Security & Privacy in the Internet of Things*. Copper Horse Ltd. Retrieved August 14, 2020, from https://iotsecuritymapping.uk/

[COS13] COSO. (2013). *Internal Control – Integrated Framework, Executive Summary*. Committee of Sponsoring Organizations of the Treadway Commission. Retrieved January 10, 2019, from https://na.theiia.org/standards-guidance/topics/Documents/Executive_Summary.pdf

[COS17] COSO. (2017). *Enterprise Risk Management – Integrating with Strategy and Performance, Executive Summary*. Committee of Sponsoring Organizations of the Treadway Commission. Retrieved January 10, 2019, from https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

[Cou17] Council of the European Union. (2017). *Proposal for Cybersecurity Act. European Union*. Retrieved February 17, 2019, from http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf

[Cra18] Craig, J. (2018). Cybersecurity Research—Essential to a Successful Digital Future. *Engineering, 4* (1), 9-10. doi: 10.1016/j.eng.2018.02.006

[Cro13] Crown. (2013). *UK CYBER SECURITY STANDARDS Research Report*. Department for Business, Innovation and Skills. Retrieved May 30, 2019, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf

[Cro17] Cross, J. (2017). ISO 31010 Risk assessment techniques and open systems. In *Proceedings of the Sixth workshop on open systems Dependability (WOSD)* (pp. 15-18), Tokyo, Japan.

[Cro18] Crown. (2018). *NIS Guidance Collection*. National Cyber Security Centre. Retrieved February 12, 2019, from https://www.ncsc.gov.uk/guidance/nis-guidance-collection

[Cro19] Crown. (2019). *Cyber Security Breaches Survey 2019*. Department for Digital, Culture, Media & Sport. Retrieved August 8, 2019, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

[CRS20] CRS. (2020). *The Internet of Things (IoT): An Overview*. Congressional Research Service. Retrieved April 2, 2021, from https://crsreports.congress.gov/product/pdf/IF/IF11239

[CSA15] CSA. (2015). *Security Guidance for Early Adopters of the Internet of Things (IoT)*. Cloud Security Alliance. Retrieved January 05, 2021, from https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

[CSA16] CSA. (2016). *Identity and Access Management for the Internet of Things - Summary Guidance*. Cloud Security Alliance. Retrieved January 05, 2021, from https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf

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

[CSA19b] CSA. (2019b). *Guide to the CSA Internet of Things (IoT) Security Controls Framework*. Cloud Security Alliance. Retrieved May 06, 2020, from https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework/

[CSA19c] CSA Singapore and MEAC of the Netherlands. (2019c). *The IoT Security Landscape – Adoption and Harmonization of Security Solutions for the Internet of Things*. Cyber Security Agency of Singapore and Ministry of Economic Affairs and Climate Policy of the Netherlands. Retrieved May 06, 2020, from https://www.csa.gov.sg/news/publications/iot-security-landscape

[CSC16] CSCC. (2016). *Cloud Security Standards: What to Expect & What to Negotiate Version 2.0*. Cloud Standards Customer Council. Retrieved January 10, 2019, from https://www.omg.org/cloud/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf

[CSD19] CSDE. (2019). *The C2 Consensus on IoT Device Security Baseline Capabilities*. Council to Secure the Digital Economy. Retrieved July 23, 2020, from https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

[Cur+16] Curley, M., Kenneally, J., & Carcary, M. (Eds.). (2016). *IT Capability Maturity Framework TM (IT-CMF TM) The Body of Knowledge Guide* (2nd ed.). Zaltbommel: Van Haren Publishing.

[CTI21] CTIA. (2021). *CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.2.2*. CTIA Certification. Retrieved March 19, 2021, from https://www.ctia.org/about-ctia/test-plans/

[Dav16] Davies, J. (2016). *ITIL Foundation All-in-One Exam Guide*. New York: McGraw-Hill Education.

[DCM18a] DCMS. (2018a). *Code of Practice for Consumer IoT Security*. United Kingdom Department for Digital, Culture, Media and Sport. Retrieved August 14, 2020, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

[DCM18b] DCMS. (2018b). *Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security*. United Kingdom Department for Digital, Culture, Media and Sport. Retrieved August 14, 2020, from 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

[DCM21] DCMS. (2021). *New cyber security laws to protect smart devices amid pandemic sales surge*. United Kingdom Department for Digital, Culture, Media and Sport. Retrieved June 8, 2021, from https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge

[Del12] Deloitte. (2012). *ISO27032: Guidelines for cyber security A Deloitte point of view on analysing & implementing the guideline*. Deloitte LLP. Retrieved January 10, 2019, from https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/iso27032_guidelines_cybersecurity_2011_deloitte_uk.pdf

[Del17a] Deloitte. (2017a). *The value of visibility Cybersecurity risk management examination*. Deloitte Development LLC. Retrieved January 10, 2019, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-the-value-of-visibility-cybersecurity-risk-management-examination.pdf

[Del17b] Deloitte. (2017b). *Global cybersecurity compliance integrity*. Deloitte Development LLC. Retrieved February 17, 2019, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-global-cybersecurity-compliance-integrity.pdf

[Del18a] Deloitte. (2018a). *Cyber risk and regulation in Europe A new paradigm form banks*. Deloitte LLP. Retrieved January 10, 2019, from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cyber-risk-and-regulation-in-europe.pdf

[Del18b] Deloitte. (2018b). *Data and records disposition under new cybersecurity regulations: Is your organization ready?* Deloitte Development LLC. Retrieved January 10, 2019, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-regulatory-data-disposition-nyfds-cybersecurity.pdf

[Del20] Deloitte. (2020). *Internet of Things (IoT) The rise of the connected world*. Deloitte Touche Tohmatsu India LLP. Retrieved April 2, 2021, from https://www2.deloitte.com/in/en/pages/technology-media-and-telecommunications/articles/iot-2020.html

[Dep18] Department of Homeland Security. (2018). *Cyber Resilience Review (CRR)*. Department of Homeland Security. Retrieved January 10, 2019, from https://www.us-cert.gov/ccubedvp/assessments

[Deu+14] Deutscher, S., Bohmayr, W., Yin, W., & Russo, M. (2014). *Cybersecurity Meets IT Risk Management A Corporate Immune and Defense System*. Boston Consulting Group. Retrieved January 10, 2019, from https://www.bcg.com/publications/2014/technology-strategy-organization-cybersecurity-meets-it-risk-management.aspx

[DHS16] DHS. (2016). *Strategic Principles for Securing the Internet of Things (IoT) Version 1.0*. US Department of Homeland Security. Retrieved July 20, 2020, from https://www.dhs.gov/securingtheIoT

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

[DLA18] DLA Piper. (2018). *Data protection laws of the world*. DLA Piper. Retrieved November 19, 2018, from https://www.dlapiperdataprotection.com

[Doy14] Doyle, C. (2014). *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*. Congressional Research Service. Retrieved February 05, 2019, from https://fas.org/sgp/crs/misc/97-1025.pdf

[ECS17] ECSO. (2017). *State of the Art Syllabus v1 Overview of existing Cybersecurity standards and certification schemes*. European Cyber Security Organization. Retrieved July 20, 2020, from http://www.ecs-org.eu/documents/uploads/state-of-the-art-syllabus-v1.pdf

[ENI06] ENISA. (2006). *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*. European Network and Information Security Agency. Retrieved January 10, 2019, from https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools/at_download/fullReport

[ENI08] ENISA. (2008). *Integration of Risk Management / Risk Assessment into Business Governance, Project Report*. European Network and Information Security Agency. Retrieved January 10, 2019, from https://www.enisa.europa.eu/publications/archive/integration-of-rm-ra-into-business-governance/at_download/fullReport

[ENI13] ENISA. (2013). *Task Forces on Terminology Definitions and Categorisation of Assets (TF-TDCA)*. The European Union Agency for Cybersecurity. Retrieved February 23, 2021, from https://www.enisa.europa.eu/publications/tf-tdca

[ENI15] ENISA. (2015). *Information security and privacy standards for SMEs*. European Network and Information Security Agency. Retrieved January 10, 2019, from https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport

[ENI16a] ENISA. (2016a). *ENISA's Position on the NIS Directive*. European Network and Information Security Agency. Retrieved January 10, 2019, from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-position-on-the-nis-directive/

[ENI16b] ENISA. (2016b). *Threat Taxonomy*. European Union Agency for Cybersecurity. Retrieved August 9, 2019, from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy

[ENI17a] ENISA. (2017a). *ENISA overview of cybersecurity and related terminology*. European Network and Information Security Agency. Retrieved January

10, 2019, from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

[ENI17b] ENISA. (2017b). *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*. The European Union Agency for Cybersecurity. Retrieved July 20, 2020, from https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[ENI18a] ENISA. (2018a). *ENISA Threat Landscape Report 2017*. European Union Agency for Cybersecurity. Retrieved August 06, 2019, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport

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

[ENI19a] ENISA. (2019a). *ENISA Threat Landscape Report 2018*. European Union Agency for Cybersecurity. Retrieved August 06, 2019, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[ENI19b] ENISA. (2019b). *Good Practices for Security of IoT Secure Software Development Lifecycle*. The European Union Agency for Cybersecurity. Retrieved January 05, 2021, from https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

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

[ENI20b] ENISA. (2020b). *Guidelines for Securing the Internet of Things Secure supply chain for IoT*. The European Union Agency for Cybersecurity. Retrieved January 11, 2021, from https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[ETS17] ETSI. (2017). *CYBER; Global Cyber Security Ecosystem*. European Telecommunications Standards Institute. Retrieved January 10, 2019, from https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.02.01_60/tr_103306v010201p.pdf

[ETS20] ETSI. (2020). *ETSI European Standard (EN) 303.645 Cyber Security for Consumer Internet of Things: Baseline Requirements*. European Telecommunications Standards Institute. Retrieved July 21, 2020, from https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[Eur17] Europol. (2017). *INTERNET ORGANISED CRIME THREAT ASSESSMENT 2017*. European Union Agency for Law Enforcement Cooperation. Retrieved January 10, 2019, from https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf

[Eur18] Europol. (2018). *Internet Organised Crime Threat Assessment (IOCTA) 2018*. European Union Agency for Law Enforcement Cooperation. Retrieved August 7, 2019, from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

[Eur18a] European Union. (2018a). *Regulations, Directives and other acts*. *European Union*. Retrieved February 09, 2019, from https://europa.eu/european-union/eu-law/legal-acts_en

[Eur18b] European Union. (2018b). *The GDPR: new opportunities, new obligations*. Luxembourg: Publications Office of the European Union.

[Eur19] European Union. (2019). *Data protection reform*. European Union. Retrieved February 03, 2019, from https://www.consilium.europa.eu/en/policies/data-protection-reform/

[Eur20] European Union. (2020). *IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins)*. Publications Office of the European Union. Retrieved April 2, 2021, from https://ec.europa.eu/jrc/en/publication/iot-20-and-internet-transformation-web-things-and-digital-twins

[Eur, n.d.] European Commission. (n.d.). *SME definition*. European Commission. Retrieved June 12, 2021, from https://ec.europa.eu/growth/smes/sme-definition_en

[EY14] EY. (2014). *Cyber program management Identifying ways to get ahead of cybercrime*. EY. Retrieved January 10, 2019, from https://www.ey.com/Publication/vwLUAssets/EY-cyber-program-management/$FILE/EY-cyber-program-management.pdf

[EY17a] EY. (2017a). Governing cyber risk in financial services. pp 2-7.

[EY17b] EY. (2017b). *Payment Services Directive 2 for FinTech & Payment Service Providers Accelerate your growth journey*. EY. Retrieved January 10, 2019, from https://www.ey.com/Publication/vwLUAssets/HVG-payment-services-directive-2/$FILE/HVG-payment-services-directive-2.pdf

[EY17c] EY. (2017c). *Networking and Information Security (NIS) Directive An outline of consequences and next steps*. EY. Retrieved January 10, 2019, from https://www.ey.com/Publication/vwLUAssets/EY-networking-and-information-security-directive-nis/$FILE/EY-networking-and-information-security-directive-nis.pdf

[EY17d] EY. (2017d). *Cybersecurity requirements for financial services companies Overview of the finalized Cybersecurity Requirements from the New York State Department of Financial Services (DFS)*. EY. Retrieved January 10, 2019, from https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-requirements-for-financial-services-companies/$FILE/EY-cybersecurity-requirements-for-financial-services-companies.pdf

[EY18a] EY. (2018a). *Cybersecurity regained: preparing to face cyber attacks 20th Global Information Security Survey 2017–18*. EY. Retrieved January 10, 2019, from https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf

[EY18b] EY. (2018b). *Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19*. EY. Retrieved August 6, 2019, from https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf

[EY20] EY. (2020). *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*. EYGM Limited. Retrieved April 2, 2021, from https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-report.pdf

[Fer+17] Ferdinand, J., & Benham, R. (2017). *The Cyber Security Ecosystem: Defining A Taxonomy of Existing, Emerging and Future Cyber Threats*. SWIFT Institute. Retrieved August 8, 2019, from https://swiftinstitute.org/wp-content/uploads/2017/10/SIWP-2016-002_Cyber-Taxonomy_-Ferdinand-Benham-_vfinal2.pdf

[Fer+18] Fergusson, I. F., & Kerr, P.K. (2018). *The U.S. Export Control System and the Export Control Reform Initiative*. Congressional Research Service. Retrieved February 02, 2019, from https://fas.org/sgp/crs/natsec/R41916.pdf

[Fir+17] FireEye and Marsh & McLennan Companies. (2017). *Cyber Risk Report 2017 Cyber Threats: A perfect storm about to hit Europe?* FireEye, Inc. and Marsh & McLennan Companies. Retrieved February 09, 2019, from http://probroker.marshbrokernetworks.com/media/1201/cyber_threats_uk.pdf

[Fis14] Fischer, E.A. (2014). *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*. Congressional Research Service. Retrieved January 23, 2019, from https://fas.org/sgp/crs/natsec/R42114.pdf

[Fle+88] Flemming, N.C., & Max, M.D. (1988). Code of practice for scientific diving: Principles for the safe practice of scientific diving in different environments. Paris: United Nations Educational, Scientific and Cultural Organization (UNESCO). *UNESCO Technical Papers in Marine Science, 53*.

[For21] Forescout Technologies. (2021). *The Enterprise of Things Security Report The State of IoT Security. Forescout Technologies*. Retrieved June 07, 2021, from https://www.forescout.com/the-enterprise-of-things-security-report-state-of-iot-security-in-2020/

[Fre+15] Freund, J., & Jones, J. (2015). *Measuring and Managing Information Risk A FAIR Approach*. Oxford: Elsevier.

[Fri+10] Frippiat, D., & Marquis, N. (2010). Web Surveys in the Social Sciences: An Overview. *Population, 65*, 285-311. https://doi.org/10.3917/popu.1002.0309

[Ful17] Fulford, E. (2017). What factors influence companies' successful implementations of technology risk management systems? *Muma Business Review, 1* (13), 157-169.

[Gar+19] Garcia-Morchon, O., Kumar, S., & Sethi, M. (2019). Internet of Things (IoT) Security: State of the Art and Challenges. *Internet Research Task Force (IRTF), RFC 8576*. doi: 10.17487/RFC8576

[Gas+17] Gashgari, G., Walters, R.J., & Wills, G. (2017). A Proposed Best-practice Framework for Information Security Governance. In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)* (pp. 295-301). doi: 10.5220/0006303102950301

[Gay+18] Gayialis, S.P., Konstantakopoulos, G.D., Kechagias, E.P., Papadopoulos, G.A., & Ponis, S.T. (2018). Developing an advanced cloud-based vehicle routing and scheduling system for urban freight transportation. In I. Moon, G. Lee, J. Park, D. Kiritsis & G. Von Cieminski (Eds.), *Advances in Production Management Systems. Smart Manufacturing for Industry 4.0* (Vol. 536, pp. 190–197). Cham, Switzerland: Springer.

[Gay+20] Gayialis, S.P., Konstantakopoulos, G.D., Kechagias, E.P., & Papadopoulos, G.A. (2020). An Advanced Transportation System Based on Internet of Things. In *Proceedings of the 10th Annual International Conference on Industrial Engineering and Operations Management (IEOM 2020)* (pp. 3007-3012). Dubai, United Arab Emirates, March 10-12, 2020. ISSN: 2169-8767, ISBN: 978-1-5323-5952-1.

[Gem18] Gemalto. (2018). *The State of IoT Security*. Gemalto. Retrieved June 07, 2021, from https://www.infopoint-security.de/media/gemalto-state-of-iot-security-report.pdf

[Gha+10] Ghauri, P., & Gronhaug, K. (2010). *Research Methods in Business Studies* (4th ed.). Essex: Pearson Education Limited.

[Gha+14] Ghazouani, M., Faris, S., Medromi, H., & Sayouti, A. (2014). Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk. *International Journal of Computer Applications, 103* (4), 36-42. doi: 10.5120/18097-9155

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

[Gje+11] Gjerdrum, D., & Peter, M. (2011). The new international standard on the practice of risk management - a comparison of ISO 31000:2009 and the COSO ERM framework. *Society of Actuaries*, Issue 21

[Glo17] Global Legal Group. (2017). *The International Comparative Legal Guide to: Cybersecurity 2018.* (1st ed.). London: Global Legal Group Ltd.

[Gov03] Government of Singapore. (2003). *Strategic goods (control) act (chapter 300)*. Government of Singapore. Retrieved February 08, 2019, from https://sso.agc.gov.sg/Act/SGCA2002

[Gov07] Government of Singapore. (2007). *Computer misuse act (chapter 50a)*. Government of Singapore. Retrieved February 08, 2019, from https://sso.agc.gov.sg/Act/50A

[Gov12] Government of Singapore. (2012). *Personal data protection act 2012*. Government of Singapore. Retrieved February 08, 2019, from https://sso.agc.gov.sg/Act/PDPA2012

[Gov16] Government of Singapore. (2016). *Singapore's Cybersecurity Strategy*. Government of Singapore. Retrieved February 06, 2019, from https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

[Gov18] Government of Singapore. (2018). *Cybersecurity Act 2018*. Government of Singapore. Retrieved February 08, 2019, from https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312

[GSM18] GSM Association. (2018). *GSMA IoT Security Assessment Checklist Version 3.0*. GSM Association. Retrieved July 13, 2020, Available: https://www.gsma.com/iot/iot-security-assessment/

[GSM19] GSMA. (2019). *Mobile Telecommunications Security Threat Landscape*. GSMA. Retrieved August 8, 2019, from https://www.gsma.com/aboutus/resources/mobile-telecommunications-security-threat-landscape

[Häg+17] Häger, E.W., & Dackö, C. (2017). *Cybersecurity Law Overview*. Stockholm: Mannheimer Swartling.

[Has+20] Hassan, R., Qamar, F., Hasan, M.K., Aman, A.H.M., & Ahmed, A.S. (2020). Internet of Things and Its Applications: A Comprehensive Survey. *Symmetry*, *12*, 1674. https://doi.org/10.3390/sym12101674

[Hat+15] Hathaway, M., et al. (2015). *Cyber readiness index 2.0*. Potomac Institute for Policy Studies. Retrieved November 19, 2018, from http://www.potomacinstitute.org/academic-centers/cyber-readiness-index

[HFS19] HFS Research. (2019). *HFS Top 10 Internet of Things (IoT) Service Providers 2019*. HFS Research Ltd. Retrieved April 9, 2021, from 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

[Hog18] Hogan Lovells. (2018). *Asia Pacific Data Protection and Cyber Security Guide 2018*. Hogan Lovells. Retrieved February 07, 2019, from https://www.hoganlovells.com/

[IAP19] IAPP. (2019). *IAPP-OneTrust Research: Bridging ISO 27001 to GDPR*. International Association of Privacy Professionals. Retrieved February 12, 2019, from https://iapp.org/resources/article/iapp-onetrust-research-bridging-iso-27001-to-gdpr/

[IBM18a] IBM Security. (2018a). *IBM X-Force Threat Intelligence Index 2018 Notable security events of 2017, and a look ahead*. IBM Corporation. Retrieved January 10, 2019, from https://public.dhe.ibm.com/common/ssi/ecm/77/en/77014377usen/security-ibm-security-solutions-wg-research-report-77014377usen-20180404.pdf

[IBM18b] IBM. (2018b). *Electronics Industrial IoT cybersecurity*. IBM Corporation. Retrieved June 07, 2021, from https://www.ibm.com/thought-leadership/institute-business-value/report/electronicsiiot

[IBM19] IBM. (2019). *2019 IBM X-Force Threat Intelligence Index Report*. IBM Corporation. Retrieved August 7, 2019, from https://www.ibm.com/security/data-breach/threat-intelligence

[ICO18] ICO. (2018). *Guide to the General Data Protection Regulation (GDPR)*. Information Commissioner's Office. Retrieved February 09, 2019, from https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

[IEC16] IEC. (2016). *IoT 2020: Smart and secure IoT platform*. International Electrotechnical Commission. Retrieved April 2, 2021, from https://basecamp.iec.ch/download/iec-white-paper-iot-2020-smart-and-secure-iot-platform/

[IEC18] IEC. (2018). *Developing International Standards*. International Electrotechnical Commission (IEC). Retrieved January 10, 2019, from http://www.iec.ch/about/activities/standards.htm

[IEE17] IEEE. (2017). *Internet of Things (IoT) Security Best Practices*. Institute of Electrical and Electronics Engineers. Retrieved January 06, 2021, from https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_may_2017.pdf

[IET17] IETF. (2017). *CBOR Object Signing and Encryption (COSE)*. Internet Engineering Task Force. Retrieved March 19, 2021, from https://tools.ietf.org/pdf/rfc8152.pdf

[IIC16] IIC. (2016). *Industrial Internet of Things Volume G4: Security Framework*. Industrial Internet Consortium. Retrieved January 06, 2021, from https://www.iiconsortium.org/IISF.htm

[Inn10] Innotrain IT. (2010). *IT Service Management Methods and Frameworks Systematization*. Innotrain IT. Retrieved January 10, 2019, from https://docplayer.net/1412218-Innotrain-it-it-service-management-methods-and-frameworks-systematization.html

[Ion13] Ionita, D. (2013). *Current established Risk Assessment methodologies and tools*. [Master's thesis, University of Twente]. Retrieved January 10, 2019, from https://essay.utwente.nl/63830/1/MSc_D_Ionita.pdf

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

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

[IoT20b] IoTSF. (2020b). *IoT Security Compliance Questionnaire Release 2.1*. IoT Security Foundation. Retrieved July 20, 2020, from https://www.iotsecurityfoundation.org/best-practice-guidelines/

[IRM02] IRM. (2002). *A Risk Management Standard*. Institute of Risk Management. Retrieved January 10, 2019, from https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

[IRM18] IRM. (2018). *A Risk Practitioners Guide to ISO 31000: 2018*. Institute of Risk Management. Retrieved January 10, 2019, from https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf

[Irw+16] Irwin, C.W., & Stafford, E.T. (2016). *Survey methods for educators: Collaborative survey development (part 1 of 3)* (REL 2016–163). Washington, DC: US Department of Education, Institute of Education Sciences, National Center for Education Evaluation and Regional Assistance, Regional Educational Laboratory Northeast & Islands.

[ISA09] ISACA. (2009). *The Risk IT Framework Excerpt*. Information Systems Audit and Control Association. Retrieved January 10, 2019, from http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf

[ISA12] ISACA. (2012). *COBIT5 Enabling Processes*. Information Systems Audit and Control Association. Retrieved January 10, 2019, from http://www.isaca.org/COBIT/Documents/COBIT-5-Enabling-Processes-Introduction.pdf

[ISA16] ISA. (2016). *The 62443 series of standards Industrial Automation and Control Systems Security*. International Society of Automation. Retrieved January 10, 2019, from https://www.isa.org/isa99/

[ISA21] ISACA. (2021). *ISACA Glossary*. ISACA. Retrieved February 23, 2021, from https://www.isaca.org/resources/glossary#glossg

[ISF11] ISF. (2011). *The 2011 Standard of Good Practice for Information Security*. Information Security Forum. pp. 1-271.

[ISF14] ISF. (2014). *IRAM2 The next generation of assessing information risk*. Information Security Forum. pp 1-90.

[ISO09] ISO. (2009). *IEC 31010:2009 Preview Risk management -- Risk assessment techniques*. International Organization for Standardization. Retrieved January 10, 2019, from https://www.iso.org/standard/51073.html

[ISO12] ISO. (2012). *ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity*. International Organization for Standardization. Retrieved January 10, 2019, from https://www.iso.org/standard/44375.html

[ISO13a] ISO. (2013a). *ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements*. International Organization for Standardization. Retrieved January 10, 2019, from https://www.iso.org/standard/54534.html

[ISO13b] ISO. (2013b). *ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls*. International Organization for Standardization. Retrieved January 10, 2019, from https://www.iso.org/standard/54533.html

[ISO18a] ISO. (2018a). *We're ISO: we develop and publish International Standards*. International Organization for Standardization. Retrieved January 10, 2019, from https://www.iso.org/standards.html

[ISO18b] ISO. (2018b). *ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*. International Organization for Standardization. Retrieved January 10, 2019, from https://www.iso.org/standard/73906.html

[ISO18c] ISO. (2018c). *ISO/IEC 27005:2018 Information technology -- Security techniques -- Information security risk management.* International Organization for Standardization. Retrieved January 10, 2019, from https://www.iso.org/standard/75281.html

[ISO18d] ISO. (2018d). *ISO 31000:2018*. International Organization for Standardization. Retrieved January 10, 2019, from https://www.iso.org/standard/65694.html

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

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

[ITU18] ITU. (2018). *ITU-T Recommendations and other publications*. International Telecommunication Union. Retrieved January 10, 2019, from https://www.itu.int/en/ITU-T/publications/Pages/default.aspx

[Jal+18] Jalali, M.S., Siegel, M., & Madnick, S. (2018). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems, 28* (1), 66-82. https://doi.org/10.1016/j.jsis.2018.09.003

[Joh+14] Johnson, J., Lincke, S. J., Imhof, R., & Lim, C. (2014). A comparison of international information security. *Interdisciplinary Journal of Information, Knowledge, and Management*, *9*, 89-116.

[Jol19] Jolly, I. (2019). *Data protection in the United States: overview*. Thomson Reuters. Retrieved February 04, 2019, from https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1

[Jon06] Jones, J.A. (2006). *An Introduction to Factor Analysis of Information Risk (FAIR)*. Risk Management Insight LLC.

[Jun17] Juniper Research. (2017). *The Future of Cybercrime & Security: Enterprise Threats & Mitigation 2017-2022*. Juniper Research Ltd. Retrieved January 10, 2019, from https://www.juniperresearch.com/press/press-releases/cybercrime-to-cost-global-business-over-$8-trn

[Jun+18] Juniper Networks and Internet of Things Institute. (2018). *Securing IoT at Scale Requires a Holistic Approach Survey Insights Revealed by IoT Adopters*. Juniper Networks. Retrieved June 07, 2021, from https://www.juniper.net/assets/kr/kr/local/pdf/ebooks/7400082-en.pdf

[Jun20] Juniper Research. (2020). *IOT ~ THE INTERNET OF TRANSFORMATION 2020*. Juniper Research Ltd. Retrieved April 2, 2021, from https://www.juniperresearch.com/white-papers/iot-the-internet-of-transformation-2020

[Kas+21] Kashani, M.H., Madanipour, M., Nikravan, M., Asghari, P., & Mahdipour, E. (2021). A systematic review of IoT in healthcare: Applications, techniques, and trends. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2021.103164

[Kec+20] Kechagias, E.P., Gayialis, S.P., Konstantakopoulos, G.D., & Papadopoulos, G.A. (2020). An Application of an Urban Freight Transportation System for Reduced Environmental Emissions. *Systems*, *8*, 49. https://doi.org/10.3390/systems8040049

[Keu15] Keusch, F. (2015). Why do people participate in Web surveys? Applying survey participation theory to Internet survey data collection. *Management Review Quarterly, 65*, 183–216. https://doi.org/10.1007/s11301-014-0111-y

[Kha+20] Khanna, A., & Kaur, S. (2020). Internet of Things (IoT), applications and challenges: A comprehensive review. *Wireless Personal Communications*, *114*, 1687-1762. https://doi.org/10.1007/s11277-020-07446-4

[Kir+13] Kiran, K.V.D., Mukkamala, S., & Katragadda, A. (2013). Performance And Analysis Of Risk Assessment Methodologies. In *Information Security. International Journal of Computer Trends and Technology (IJCTT), 4* (10), 3685-3692.

[Kos18a] Kosseff, J. (2018a). *Developing collaborative and cohesive cybersecurity legal principles*. 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, 283-298. doi: 10.23919/CYCON.2018.8405022

[Kos18b] Kosseff, J. (2018b). Defining Cybersecurity Law. *Iowa Law Review*. *103* (985), 985-1031.

[KPM19] KPMG. (2019). *What's next: Key cyber security considerations for 2019*. KPMG LLP. Retrieved August 7, 2019, from https://advisory.kpmg.us/articles/2019/tackling-cyber-security-concerns.html

[Lab+06] Labuschagne, W.G., & Bornman, L. (2006). *A comparative framework for evaluating information security risk management methods*. Technical report. Standard Bank Academy for Information Technology, Rand Afrikaans University.

[Lal+21] Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105* (102248). https://doi.org/10.1016/j.cose.2021.102248

[Lau18] Launius, S. (2018). *Evaluation of Comprehensive Taxonomies for Information Technology Threats*. SANS Institute. Retrieved August 9, 2019, from https://www.sans.org/reading-room/whitepapers/threatintelligence/paper/38360

[Law17] Law Business Research. (2017). *The Privacy, Data Protection and Cybersecurity Law Review* (4th ed.). London: Gideon Roberton.

[Lee20] Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, *12* (9), 157. https://doi.org/10.3390/fi12090157

[Lin+18] Lindstrom, P., Rosen, M., & Pike, S. (2018). *DX Security: A Security Model for the DX Platform*. International Data Corporation (IDC).

[Liu+17] Liu, X., Zhao, M., Li, S., Zhang, F., & Trappe, W. (2017). A Security Framework for the Internet of Things in the Future Internet Architecture. *Future Internet*, *9* (3), 27. https://doi.org/10.3390/fi9030027

[Lon+12] Lonea, A.M., Popescu, D.E., & Prostean, O. (2012). The overall process taken by enterprises to manage the IaaS cloud services. In *Proceedings of the 6th European Conference on Information Systems Management and Evaluation (ECIME 2012)* (pp. 168-177). *University College Cork, Cork, Ireland, September 13-14, 2012*.

[Lon+13a] Lonea, A.M., Tianfield, H., & Popescu, D.E. (2013a). Identity Management for Cloud Computing. In V. Balas, J. Fodor & A. Várkonyi-Kóczy (Eds.), *New Concepts and Applications in Soft Computing. Studies in Computational Intelligence (*Vol. 417, pp. 175-199*)*. Berlin, Heidelberg: Springer. https://doi:10.1007/978-3-642-28959-0_11

[Lon+13b] Lonea, A. M., Popescu, D. E., & Tianfield, H. (2013b). Detecting DDoS attacks in cloud computing environment. *International Journal of Computers, Communications & Control*, *8* (1), 70– 78. https://doi.org/10.15837/ijccc.2013.1.170

[Mac+06] Mackenzie, N., & Knipe, S. (2006). Research dilemmas: Paradigms, methods and methodology. *Issues in educational research, 16* (2), 193-205.

[Mai+17] Maier, J., Eckert, C., & John Clarkson, P. (2017). Model granularity in engineering design – concepts and framework. *Design Science*, *3*, E1. doi:10.1017/dsj.2016.16

[Mar17] Marsh & McLennan Companies. (2017). *MMC Cyber Handbook 2018: Perspectives on the next wave of cyber*. Marsh & McLennan Companies. Retrieved June 3, 2019, from https://www.marsh.com/us/insights/research/mmc-cyber-handbook-2018.html

[Mav+17] Mavroeidis, V., & Bromander, S. (2017). Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. In *2017 European Intelligence and Security Informatics Conference (EISIC)* (pp. 91-98). IEEE, Athens. doi: 10.1109/EISIC.2017.20.

[May18] Mayer Brown. (2018). *2018 Outlook: Cybersecurity and Data Privacy*. The Mayer Brown Practices. Retrieved November 19, 2019, from https://www.mayerbrown.com/2018-outlook-cybersecurity-and-data-privacy-01-29-2018/

[McK17] McKinsey & Company. (2017). *How CEOs can tackle the challenge of cybersecurity in the age of the Internet of Things*. McKinsey & Company. Retrieved April 2, 2021, from https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age

[McK19] McKinsey & Company. (2019). *Growing opportunities in the Internet of Things*. McKinsey & Company. Retrieved April 4, 2021, from https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things

[McK20a] McKinsey & Company. (2020a). *The 5G era New horizons for advanced electronics and industrial companies*. McKinsey & Company. Retrieved April 2, 2021, from https://www.mckinsey.com/industries/advanced-electronics/our-insights/the-5g-era-new-horizons-for-advanced-electronics-and-industrial-companies

[McK20b] McKinsey & Company. (2020b). *Cybersecurity in a Digital Era Your guide to the emerging technologies revolutionising business now*. McKinsey & Company. Retrieved April 2, 2021, from https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-in-a-digital-era

[Mes+17] Meszaros, J., & Buchalcevova, A. (2017). Introducing OSSF: A framework for online service cybersecurity risk management. *Computers & Security, 65*, 300-313. doi: 10.1016/j.cose.2016.12.008

[Mom21] Momentive. (2021). *How to Create a Survey*. Momentive. Retrieved June 9, 2021, from https://help.surveymonkey.com/articles/en_US/kb/How-to-create-a-survey

[Moo+17] Moore, K., Barnes, R., & Tschofenig, H. (2017). *Best Current Practices for Securing Internet of Things (IoT) Devices*. Internet Engineering Task Force. Retrieved March 19, 2021, from https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

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

[NCS18] NCSC. (2018). *The cyber threat to UK business 2017-2018 report*. National Cyber Security Centre. Retrieved August 7, 2019, from https://www.ncsc.gov.uk/information/the-cyber-threat-to-uk-business-2017-2018-report

[NEM18] NEMA. (2018). *Cyber Hygiene Best Practices*. National Electrical Manufacturers Association. Retrieved January 07, 2021, from https://www.nema.org/standards/view/cyber-hygiene-best-practices

[Net19] Nettitude. (2019). *Effective Cyber Security Strategy*. Nettitude. Retrieved May 12, 2018, from https://info.nettitude.com/effective-cyber-security-strategy-march-2019/

[NHT16] NHTSA. (2016). *Cybersecurity Best Practices for Modern Vehicles*. US Department of Transportation National Highway Traffic Safety Administration. Retrieved January 08, 2021, from https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

[NIS04] NIST. (2004). *Federal Information Processing Standards Publication (FIPS PUB) 199: Standards for Security Categorization of Federal Information and*

Information Systems. National Institute of Standards and Technology. Retrieved May 06, 2020, from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[NIS06] NIST. (2006). *Federal Information Processing Standards Publication (FIPS PUB) 200: Minimum Security Requirements for Federal Information and Information Systems*. National Institute of Standards and Technology. Retrieved May 06, 2020, from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[NIS10] NIST. (2010). *NIST Special Publication 800-37 Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems*. National Institute of Standards and Technology. Retrieved January 10, 2019, from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf

[NIS11] NIST. (2011). *NIST Special Publication 800-39 Managing Information Security Risk Organization, Mission, and Information System View*. National Institute of Standards and Technology. Retrieved January 10, 2019, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[NIS12a] NIST. (2012a). *NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments*. National Institute of Standards and Technology. Retrieved January 10, 2019, from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

[NIS12b] NIST. (2012b). *New NIST Publication Provides Guidance for Computer Security Risk Assessments*. National Institute of Standards and Technology. Retrieved January 10, 2019, from https://www.nist.gov/news-events/news/2012/09/new-nist-publication-provides-guidance-computer-security-risk-assessments

[NIS13] NIST. (2013). *NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations*. National Institute of Standards and Technology. Retrieved January 10, 2019, from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

[NIS14] NIST. (2014). *NIST Special Publication 800-53A Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. National Institute of Standards and Technology. Retrieved January 10, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

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

[NIS18b] NIST. (2018b). *NIST Special Publication 800-37 Revision 2 Risk Management Framework for Information Systems and Organizations*. National Institute of Standards and Technology. Retrieved March 05, 2021, from https://doi.org/10.6028/NIST.SP.800-37r2

[NIS19a] NIST. (2019a). *Glossary*. National Institute of Standards and Technology. Retrieved August 17, 2019, from https://csrc.nist.gov/glossary

[NIS19b] NIST. (2019b). *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. National Institute of Standards and Technology. Retrieved July 24, 2020, from https://doi.org/10.6028/NIST.IR.8228

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

[NIS20b] NIST. (2020b). *IoT Device Cybersecurity Capability Core Baseline*. National Institute of Standards and Technology. Retrieved January 07, 2021, from https://doi.org/10.6028/NIST.IR.8259A

[Nur+17] Nurse, J.R.C., Creese, S., & De Roure, D. (2017). Security Risk Assessment in Internet of Things Systems. *IT Professional, 19* (5), 20-26. https://doi: 10.1109/MITP.2017.3680959

[Off08] Official Journal of the European Union. (2008). *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. Official Journal of the European Union. Retrieved February 03, 2019, Available: https://eur-lex.europa.eu/

[Off09] Official Journal of the European Union. (2009). *Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items*. Official Journal of the European Union. Retrieved February 05, 2019, from https://eur-lex.europa.eu/

[Off13] Official Journal of the European Union. (2013). *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*. Official Journal of the European Union. Retrieved February 06, 2019, from https://eur-lex.europa.eu/

[Off16a] Official Journal of the European Union. (2016a). *General Data Protection Regulation (Regulation (EU) 2016/679) of 27 April 2016*. Official Journal of the European Union. Retrieved February 03, 2019, from https://eur-lex.europa.eu/

[Off16b] Official Journal of the European Union. (2016b). *Directive (EU) 2016/680 of 27 April 2016*. Official Journal of the European Union. Retrieved February 03, 2019, from https://eur-lex.europa.eu/

[Off16c] Official Journal of the European Union. (2016c). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Official Journal of the European Union. Retrieved February 03, 2019, from https://eur-lex.europa.eu/

[one18] oneM2M. (2018). *TR-0008-V2.0.1 Security* (Technical Report). oneM2M Partners Type 1. Retrieved March 19, 2021, from https://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf

[Ora19] Oracle. (2019). *Oracle and KPMG Cloud Threat Report 2019 Defining Edge Intelligence: Closing Visibility Gaps with a Layered Defense Strategy*. Oracle. Retrieved August 8, 2019, from https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2019/cloud-threat-report-2019-oracle-kpmg.pdf

[OTA18] OTA. (2018). *IoT Security & Privacy Trust Framework v2.5*. Online Trust Alliance. Retrieved July 22, 2020, from https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/

[OWA10] OWASP. (2010). *OWASP Secure Coding Practices Quick Reference Guide*. The OWASP Foundation. Retrieved March 19, 2021, from https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf

[OWA19] OWASP. (2019). *OWASP Risk Rating Methodology*. Open Web Application Security Project. Retrieved September 12, 2019, from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[Pal20] Palo Alto Networks. (2020). *2020 Unit 42 IoT Threat Report*. Palo Alto Networks. Retrieved June 7, 2021, from https://start.paloaltonetworks.com/unit-42-iot-threat-report

[Pal+03] Palvia, P., Mao, E., Salam, A.F., & Soliman, K.S. (2003). Management Information Systems Research: What's There in a Methodology? *Communications of the Association for Information Systems, 11* (16), 289–309.

[PDP17] PDPC. (2017). *Advisory guidelines on key concepts in the personal data protection act*. Government of Singapore. Retrieved February 08, 2019, from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-key-concepts-in-the-pdpa-(270717).pdf

[Per+16] Pernik, P., Wojtkowiak, J., & Verschoor-Kirss, A. (2016). *National Cyber Security Organisation: UNITED STATES*. The NATO Cooperative Cyber Defence Centre of Excellence. Retrieved November 28, 2018, from https://ccdcoe.org/multimedia/national-cyber-security-organisation-usa.html

[Pon18] Ponemon Institute. (2018). *2018 Study on global megatrends in cybersecurity*. Ponemon Institute LLC*.* Retrieved November 19, 2018, from https://www.raytheon.com/cyber/cyber_megatrends

[Pon19] Ponemon Institute. (2019). *The Cybersecurity Illusion: Enterprise Security Remains Reactive*. Ponemon Institute. Retrieved January 8, 2020, from https://go.attackiq.com/rs/041-FSQ-281/images/REPORT-Ponemon2_v2.pdf

[Pon20] Ponemon Institute. (2020). *A New Roadmap for Third Party IoT Risk Management The Critical Need to Elevate Accountability, Authority and Engagement*. Ponemon Institute and The Santa Fe Group, Shared Assessments Program. Retrieved April 2, 2021, from https://sharedassessments.org/blog/a-new-roadmap-for-third-party-iot-risk-management/

[Poo+04] Poon, P.S., Albaum, G., & Evangelista, F.U. (2004). Why People Respond to Surveys. *Journal of International Consumer Marketing, 16*, 75-90. https://doi.org/10.1300/J046v16n02_05

[Pop+18] Poppensieker, T., & Riemenschnitter, R. (2018). *A new posture for cybersecurity in a networked world*. McKinsey & Company. Retrieved January 10, 2019, from https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world

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

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

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

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

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

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

[PSA21] PSA JSA Members. (2021). *PSA Certified™ Level 1 Questionnaire, Version 2.1*. Arm Limited. Retrieved March 19, 2021, from https://www.psacertified.org/getting-certified/device-manufacturer/level-1/

[PwC16] PwC. (2016). *10 most likely ways your operational technology network will be compromised December 2015 Cyber savvy: Securing operational technology assets*. PwC. Retrieved January 10, 2019, from https://www.pwc.com/ca/en/consulting/publications/2016-01-18-pwc-cyber-savvy-securing-operational-technology-assets.pdf

[PwC17] PwC. (2017). *Top financial services issues of 2018*. PwC. Retrieved January 10, 2019, from https://www.pwc.se/sv/pdf-reports/finansiell-sektor/top-financial-services-issues-of-2018.pdf

[PwC18] PwC. (2018). *Revitalizing privacy and trust in a data-driven world Key findings from The Global State of Information Security® Survey 2018*. PwC. Retrieved January 10, 2019, from https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

[R+18] R, J., & Chandran, P. (2018). Secure and Dynamic Memory Management Architecture for Virtualization Technologies in IoT Devices. *Future Internet*, *10* (12), 119. https://doi.org/10.3390/fi10120119

[Rav+18] Ravishankar, V., Mooney, O., & Hader, N., (2018). *Stepping up governance on cyber security what is corporate disclosure telling investors?* PRI Association. Retrieved November 27, 2018, from https://www.unpri.org/governance-issues/corporate-disclosure-on-cyber-security-governance-processes-and-procedures-/3462.article

[Rey+19] Reyna, J., Hanham, J., Vlachopoulos, P., & Meier, P. (2019). Using factor analysis to validate a questionnaire to explore self-regulation in learner-generated digital media (LGDM) assignments in science education. *Australasian journal of educational technology*, *35*, 128-152. https://doi.org/10.14742/ajet.4514

[Rod14] Rodion, Z. (2014). *Analysis of information risk management methods.* [Bachelor's Thesis, University of Jyväskylä]. Retrieved May 30, 2019, from https://jyx.jyu.fi/bitstream/handle/123456789/43760/1/Rodion%20Zudin.pdf

[Rog+16] Rogers, B.E., & Dunkerley, D. (2016). *CRISC™ Certified in Risk and Information Systems Control All-in-One Exam Guide*. New York: McGraw-Hill Education.

[Ros+16] Ross, R., McEvilley, M., & Carrier Oren, J. (2016). *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. National Institute of Standards and Technology. Retrieved March 19, 2021, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

[UL19] UL. (2019). *Security concerns escalate as IoT expands Market insights on the state of IoT security*. UL. Retrieved June 07, 2021, from https://www.ul.com/sites/g/files/qbfpbp251/files/2019-04/security-concerns-escalate-as-iot-expands.pdf

[Sán+12] Sánchez-Fernández, J., Muñoz-Leiva, F., & Montoro-Ríos, F.J. (2012). Improving retention rate and response quality in Web-based surveys. *Computers in Human Behavior, 28*, 507-514. https://doi.org/10.1016/j.chb.2011.10.023

[San18] SANS Institute. (2018). *The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns*. SANS Institute. Retrieved June 07, 2021, from https://www.forescout.com/2018-sans-industrial-iot-security-survey/

[Sch87] Schwaninger, M. (1987). A Practical Approach to Strategy Development. Long Range Planning, 20 (5), 74-85. https://doi.org/10.1016/0024-6301(87)90094-X

[Sec19] Secureworks. (2019). *2019 Incident Response Insights Report A Case for Mastering Security Fundamentals*. Secureworks. Retrieved August 8, 2019, from https://www.secureworks.com/resources/rp-incident-response-insights-report-2019

[SEI07] SEI. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Technical Report. *Software Engineering Institute*. Retrieved January 10, 2019, from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

[Sha+16a] Shameli-Sendi,A., Aghababaei-Barzegar, R., & Cheriet, M. (2016a). Taxonomy of information security risk assessment (ISRA). *Comput. Secur*., *57*, C (March 2016), 14–30. https://doi.org/10.1016/j.cose.2015.11.001

[Sha+16b] Shackelford, S.J., Russell, S., & Haut, J. (2016b). Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks. *UC Davis Business Law Journal*, *16* (2), 217-260.

[She+05] Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise Security Architecture A Business-Driven Approach*. Boca Raton*:* Taylor & Francis Group.

[She+09] Sherwood, J., Clark, A., & Lynas, D. (2009). *Enterprise Security Architecture. White Paper*. SABSA Limited*.*

[She+18] Shevchenko, N., et al. (2018). *Threat Modeling: A Summary of Available Methods*. Software Engineering Institute. Retrieved September 6, 2019, from https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf

[Sho14] Shostack, A. (2014). *Threat Modeling: Designing for Security*. Indianapolis, Indiana: Wiley.

[Sin16] Singapore's Ministry of Home Affairs. (2016). *National Cybercrime Action Plan (NCAP)*. Government of Singapore. Retrieved February 07, 2019, from https://www.mha.gov.sg/newsroom/press-release/news/launch-of-the-national-cybercrime-action-plan

[Sin+20] Singh, R.P., Javaid, M., Haleem, A., & Suman, R. (2020). Internet of things (IoT) applications to fight against COVID-19 pandemic. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, *14* (4), 521-524. https://doi.org/10.1016/j.dsx.2020.04.041

[Sir+18] Sirur, S., Nurse, J.R., & Webb, H. (2018). Are We There Yet?: Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (MPS '18)* (pp. 88-95). Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3267357.3267368

[Sto21] Stone, M. (2021). *What is a cybersecurity strategy and how can your business develop one?* AT&T Cybersecurity. Retrieved September 04, 2021, from https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained

[Sun+18] Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018). Cybersecurity Policy in ASEAN Countries. In *17th Annual Security Conference - Securing the interconnected world*, Las Vegas.

[Sym19] Symantec. (2019). *ISTR Internet Security Threat Report Volume 24*. Symantec. Retrieved August 7, 2019, from https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

[Tal+13] Talabis, M.R.M., & Martin, J.L. (2013). Chapter 2 - Information Security Risk Assessment: A Practical Approach. In M.R.M. Talabis & J.L. Martin (Eds.), *Information Security Risk Assessment Toolkit* (pp. 27-62). Syngress.

[Tar+15] Tarala, J., & Tarala, K.K. (2015). *Open Threat Taxonomy version 1.1*. Enclave Security. Retrieved August 9, 2019, from http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf

[Tau14] Taubenberger, S. (2014). *Vulnerability Identification Errors in Security Risk Assessments*. [PhD thesis, The Open University]. https://doi.org/10.21954/ou.ro.00009aca

[Tha18] Thales. (2018). *2019 Thales Data Threat Report – Global Edition*. Thales. Retrieved August 7, 2019, from https://www.thalesesecurity.com/2019/data-threat-report

[The13] The Open Group. (2013). *Risk Taxonomy (O-RT), Version 2.0 Technical Standard*. The Open Group. Retrieved January 10, 2019, from https://publications.opengroup.org/c13k

[The13a] The White House. (2013a). *Improving critical infrastructure cybersecurity*. The White House. Retrieved February 04, 2019, from https://www.dhs.gov/sites/default/files/publications/EO-13636-Improving-Critical-Infrastructure-Cybersecurity-508.pdf

[The13b] The White House. (2013b). *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*. The White House. Retrieved February 04, 2019, from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[The17] The White House. (2017). *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. The White House. Retrieved February 04, 2019, from https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[Tre18] Trend Micro. (2018). *Mapping the Future: Dealing With Pervasive and Persistent Threats*. Trend Micro. Retrieved August 7, 2019, from https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019

[Tru18] Trustwave. (2018). *Trustwave Global Security Report*. Trustwave Holdings, Inc. Retrieved August 24, 2019, from https://www.singtel.com/content/dam/singtel/business/globalservices/Featured%20 Articles/2018-Trustwave-Global-Security-Report.pdf

[Twe+18] Tweneboah-Koduah, S., & Buchanan. W.J. (2018). Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study. *The Computer Journal, 61* (9), 1389–1406. https://doi.org/10.1093/comjnl/bxy002

[Tze+11] Tzeng, G.-H., & Huang, J.-J. (2011). *Multiple Attribute Decision Making: Methods and Applications*. Boca Raton: CRC Press, Taylor & Francis Group.

[Uni14] United States Army. (2014). *Field Manual 3–38: cyber electromagnetic activities*. Kansas: US Army.

[US01] US Congress. (2001). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*. US Congress. Retrieved February 04, 2019, from https://www.congress.gov/

[US17] US Chamber of Commerce. (2017). *Transatlantic cybersecurity forging a united response to universal threats*. Washington: US Chamber of Commerce.

[US19] US Congress. (2019). *CLOUD Act*. US Congress. Retrieved February 17, 2019, from https://www.congress.gov/bill/115th-congress/house-bill/4943/text

[USC20] US Congress. (2020). *H.R.1668 - Internet of Things Cybersecurity Improvement Act of 2020*. US Congress. Retrieved June 8, 2021, from https://www.congress.gov/bill/116th-congress/house-bill/1668/text

[Van14] Van Os, R. (2014*). Comparing security architectures: defining and testing a model for evaluating and categorizing security architecture frameworks*. [Master's thesis, Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering, Sweden].

[Ver18] Verizon. (2018). *2018 Data Breach Investigations Report 11th edition*. Verizon. Retrieved January 10, 2019, from https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

[Ver18a] Verutus. (2018). *EU GPDR Compliance Criteria - Cybersecurity For Privacy (C4P) Overview*. Secure Controls Framework Council, LLC. Retrieved February 12, 2019, from https://www.securecontrolsframework.com/

[Ver19] Verizon. (2019). *2019 Data Breach Investigations Report*. Verizon. Retrieved August 6, 2019, from https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[W3C19] W3C. (2019). *Web of Things (WoT) Security and Privacy Guidelines*. World Wide Web Consortium. Retrieved July 23, 2020, from https://www.w3.org/TR/2019/NOTE-wot-security-20191106/#secure-practices-for-designing-a-thing-description

[WEF18a] WEF. (2018a). *Digital Transformation Initiative Maximizing the Return on Digital Investments*. World Economic Forum. Retrieved January 10, 2019, from http://www3.weforum.org/docs/DTI_Maximizing_Return_Digital_WP.pdf

[WEF18b] WEF. (2018b). *The Global Risks Report 2018 13th Edition*. World Economic Forum. Retrieved January 10, 2019, from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

[WEF19] WEF. (2019). *The Global Risks Report 2019 14th Edition*. World Economic Forum. Retrieved May 28, 2019, from http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

[WEF20a] WEF. (2020a). *Future Series: Cybersecurity, emerging technology and systemic risk INSIGHT REPORT*. World Economic Forum. Retrieved April 2, 2021, from http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf

[WEF20b] WEF. (2020b). *State of the Connected World 2020 Edition INSIGHT REPORT*. World Economic Forum. Retrieved April 2, 2021, from http://www3.weforum.org/docs/WEF_The_State_of_the_Connected_World_2020.pdf

[WEF21] WEF. (2021). *The Global Risks Report 2021 16th Edition INSIGHT REPORT*. World Economic Forum. Retrieved June 9, 2021, from http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

[WIS16] WISER Consortium. (2016). *D6.2 - Best Practices & Early Assessment Pilots, Final Version*. CYBERWISER.eu. Retrieved January 10, 2019, from https://www.cyberwiser.eu/content/d62-best-practices-early-assessment-pilots-final-version