NOVA SCHOOL OF BUSINESS & ECONOMICS

A Work Project, presented as part of the requirements for the Award of a Master's degree in Management from the Nova School of Business and Economics.

INTERNET OF THINGS (IOT) SECURITY REGULATIONS USING ENTERPRISE ARCHITECTURE

AN ANALYSIS MODELLING TWO IOT SECURITY FRAMEWORKS

ISABELLE KRUPP – 34213

Work project carried out under the supervision of:

Professor Paulo Jorge Coelho Faroleiro

4th of January 2021

Abstract

The increasing importance of security for the Internet of Things (IoT) is depicted throughout the paper *IoT Security Regulations using Enterprise Architecture.* The majority of surveyed IoT experts agree that the current status on IoT security is unclear. It is proposed to use Enterprise Architecture (EA) to compare two selected security frameworks by ENISA and the GSMA. The created EA models demonstrate the applicability of EA for IoT security based on the layered approach that integrates various viewpoints, elements and relations. Further, EA facilitates the distinction between IoT security frameworks proposing an improvement to the IoT security regulation landscape.

Keywords: Cyber Security, Regulation, Internet of Things, IoT Security, Enterprise Architecture, ArchiMate, ENISA, GSMA

Table of Contents

1. Introduction

‘In 2020, for the first time, there are more IoT [Internet of Things] connections (…) than there are non-IoT connections (…). Of the 21.7 billion active connected devices worldwide, 11.7 billion (or 54%) will be IoT device connections at the end of 2020. By 2025, it is expected that there will be more than 30 billion IoT connections, almost 4 IoT devices per person on average’ (Lueth, 2020). Simultaneously, companies are striving to fulfill the general security objectives ‘Confidentiality’, ‘Integrity’ and ‘Availability’, which are known as the ‘CIA triad’, the foundation of every security program (Eugen & Petrut, 2018). Due to the fast development and growth of the IoT technology, it becomes obvious that IoT related cybercrime increasingly risks having major impacts on society, economy and politics (Christou, 2018). Beyond that, the lack of international cooperation and differences between the national cyber security approaches present challenges for IoT Security (Urgessa, 2019).

A prominent example that highlights the current status quo is the malware attack on 4,000 IoT devices in 2019: a 14-year-old hacker used the malware dubbed ‘silex’ to target insecure IoT devices by removing their firewalls, network configurations and bringing them to a halt (O'Donnell, 2019). Also, the current Covid-19 pandemic has uncovered a wide range of IoT security risks due to the need to rapidly digitize while deprioritizing security: For instance, IoT botnets are deployed to routinely carry out Distributed Denial-of-service-attacks (DDoS) targeting home routers and accessing critical information (Acohido, 2020). Results of IoT cyber-attacks include loss of reputation and sensitive information as well as data thefts (Pipelinesecurity, 2020).

The objective of this paper is to explore the challenges of IoT Security by focusing on existing regulatory approaches. A depiction of current measures is presented, and two approaches are analyzed with the help of Enterprise Architecture (EA) focusing on comparing the IoT Security recommendations from a regulatory perspective to those of a self-regulatory perspective using two exemplary frameworks.

The paper's structure contains eight main chapters: In the first section, the **Literature Review** gives a brief introduction to the technology of the IoT, depicts the relevance of security for the IoT and provides an overview of current frameworks and studies. Additionally, the reader is introduced to modeling with the EA language, ArchiMate. The next section, **Research Design**, outlines the methodology, the research questions and motivation. In the chapter **Definition of Objectives of Solution,** the proposed analysis and a framework to evaluate the results are presented. Subsequently, **Design and Development** describes the modeling of the two proposed IoT Security frameworks that are then compared and evaluated in **Demonstration**. Finally, the models are validated with the help of the proposed framework in **Evaluation**. The **Conclusion and Outlook** summarizes the findings, answers the proposed research questions and points out limitations. The last chapter **Directions for Future Research** proposes the further development of the topic.

2. Literature Review

*2.*1 The IoT

In 1999, Kevin Ashton first used the terminology 'Internet of Things' and referred to the 'things' as components with which we 'interact and live' in our surroundings. In his opinion, the physical world needed to be reexamined as the technologies 'computing, internet and data-generation by smart devices' rapidly advance (Khodadadi, Dastjerdi, & Buyya, 2016). IoT is also referred to as connected devices, as the emphasis of the technology lays on devices built for specific tasks (Rosner, 2017). The possibilities of this technology range from time and money saving potentials to improvements of economic and social prosperity and increase in comfort and automation (Lee, 2019). These potentials simultaneously require high standards in security, privacy, authentication and recovery from attacks to maintain its advantages (Hassija, et al., 2019).

The IoT is not a single device itself, but is made up of sensors, remote service invocation, communication networks and the capacity to process technological events. These components

can be categorized in an application, middleware, network and sensing layer (Hassija, et al., 2019). While the technology stack is essential in understanding the IoT, the human component is still relevant in creating useful IoT applications: '(…) what IoT tries to picture is a unified network of smart objects and human beings responsible for operating them (if needed), who are capable of universally and ubiquitously communicating with each other.' (Khodadadi, Dastjerdi, & Buyya, 2016).

From a customer perspective, the IoT offers new 'value-added services' that are built on big data analytics and present a variety of new business models (Slama, Puhlmann, Morrish, & Bhatnagar, 2016). The application of IoT use cases is endless and spreads across all industries. The most critical applications, however, are to be found in the area of smart cities, smart environment, smart metering/smart grids, security and emergencies, smart retail, smart agriculture and home automation (Hassija, et al., 2019). Concurrently, emerging technologies may provide enhanced security for the IoT. These possibilities include solutions coming from the area of blockchain, fog computing, machine learning and edge computing. Hassija, et al (2019) presents further information on this topic.

2.2 Cyber Security for the IoT

Undoubtedly, rapid innovation and technological development of technologies, like the IoT, automatically convey security issues. Cyber attackers will increasingly make use of attack surfaces like cloud services and exploit the vulnerabilities of IoT devices (Dhanjani, 2015). This issue makes protective technological features like firmware security even more important in the growing IoT market (Polverini, et al., 2018). The growing market for IoT and digitization also stresses the need for secure technologies and trust between all stakeholders. Furthermore, the challenges of the IoT include a wide range of social, technical, legal, policy but also interoperability challenges. Cyber-attacks impact social, economic and political components of governments, society and businesses (Christou, 2018). IT security is of great relevance, but IoT security should be evaluated in an even more critical light, as an increasing amount of poorly

secured devices are connected to the internet. Yet, the security aspects for IoT do not receive enough attention (Chatfield & Reddick, 2019). The more services an organization uses and provides that are based on the internet, the stronger its cybersecurity efforts and commitments should be (von Solms & von Solms, 2018). According to Lee (2019), especially policy research is still lagging behind. His general recommendations include developing consistent regulatory frameworks, regulating with evidence and emphasizing international collaboration. Rosner (2017) suggests the following measures to increase IoT security: Laws and policy, contracts, market controls, self-regulation, certification and seals, best practices, norms, and technology measures. Also, Das, Kumar & Srinivas (2019) recommend a stronger use of standards by vendors, cyber security policies and the introduction of international certification. While developing regulatory approaches for IoT security, policies must, however, simultaneously encourage innovation, collaboration and engagement (Lee, 2019). Appendix D contains explanations of the mentioned terms. For more information on attack scenarios and security threats in specific layers of the IoT please refer to Hassija, et al. (2019).

2.3 Review of Existing Approaches

The following chapter presents an overview of current approaches that can be found in the context of IoT security. These approaches were carefully reviewed, and it was decided to focus on regulatory approaches from a European perspective. The European Network and Information Security Agency (ENISA) conducted thorough desktop research in their publication *Baseline Security Recommendations for IoT* that covers the most relevant approaches as marked in the table below. Secondly, to integrate a different perspective, the *Security Guidelines for IoT* by the Global System for Mobile Communications Association (GSMA) were selected. This approach constitutes a self-regulatory perspective coming from an industry organization. The table below presents the overview organizations, their publications on (IoT) security and an indication whether the approach has been analyzed and referenced by the selected frameworks. It aims to give an overview of existing measures;

however, for the sake of brevity they are not depicted in detail. Instead, it is labelled if they were considered in the studies conducted by ENISA and the GSMA.

Table 1: Overview of IoT Security Approaches

Organization	Publications and approaches	ENISA	GSMA
IoT Alliance Australia (IoTA)	IoT Code of Practice, Reference Framework, Security Guidelines, Inputs to Policy (IoT Alliance Australia, n.d.)	Analyzed and referenced by ENISA	Supports GSMA
Cloud Security Alliance (CSA)	CSA IoT Security Controls Framework (Cloud Security Alliance, 2019)	Analyzed and referenced by ENISA	
Institute of Electrical and Electronics Engineers (IEEE)	IEEE SA IoT Ecosystem Study, Draft for Architectural Framework for IoT Working Group, various standards related to the IoT as well as standards in development (IEEE Internet of Things, n.d.)	Analyzed and referenced by ENISA	
IoT Security Foundation (IOTSF)	IoT Security Compliance Framework, Best Practice, Secure Design Best Practice Guides, Reference Architectures, IoT Cybersecurity: Regulation Ready (IoT Security Foundation, n.d.)	Analyzed and referenced by ENISA	
International Organization for Standardization (ISO/IEC)	Several existing standards e.g. ISO/IEC 30141:2018 Internet of Things (IoT). – Reference Architecture, Several standards currently under development e.g.: ISO/IEC CD 27400.2 Cybersecurity – IoT security and privacy – Guidelines (ISO, n.d.)	Analyzed and referenced by ENISA	
National Institute of Standards and Technology (NIST)	US government based, IoT program support development of standards, guidelines, related tools. NISTIR 8259, NISTIR 8259A, NISTIR 8228 (NIST, n.d.)	Analyzed and referenced by ENISA	Referenced by GSMA

Overall, the ENISA framework can be categorized as a strategic framework while the GSMA represents an operational view. The following two chapters present the two selected approaches for analysis: The *Baseline Security Recommendations for IoT* by ENISA as well as *IoT Security Guidelines* by the GSMA.

2.3.1 Baseline Security Recommendations for IoT (ENISA)

Regulations are defined as the 'imposition of rules by government, backed by the use of penalties that are intended specifically to modify the economic behavior of individuals and firms in the private sector' (OECD, 2002). Frameworks can be used as the underlying structure to a set of regulations (Rabeau, n.d.).

ENISA holds the permanent mandate for the European Union to perform tasks in the area of cyber security certification, resilience and policy (ENISA, 2019). In 2017, ENISA published the *Baseline Security Recommendations for IoT* and primarily aims to give IoT security Recommendations for critical infrastructures. The document depicts the key elements of the IoT and the applied methodology, analyzes the main threats, derives security measures and challenges and concludes by presenting security recommendations (ENISA, 2017). The study is a foundation that is referenced by several further studies by ENISA: The *IoT Security Standards Gap Analysis* for instance, a study published in 2019 by ENISA, comes to the conclusion on standardization of IoT Security that even though a high number of organizations develop security standards, these also compete with each other. This incertitude in competencies creates yet another risk for security (ENISA, 2019). ENISA underlines that there are no major gaps in standardization in IoT, yet the characteristic of the IoT itself needs a more flexible and generic approach: a holistic approach to IoT security is needed. More developed approaches by ENISA include various vertical applications for IoT security like *Smart Manufacturing, Smart Hospitals* or *Smart Cars* as well as *Good Practices for Security of IoT* which targets IoT software developers and integrators (ENISA, 2019). The most recent

publication in this field is the *Guidelines for Securing the Internet of Things* giving security recommendations for the supply chain for IoT (ENISA, 2020).

2.3.2 IoT Security Guidelines (GSMA)

Industry-self-regulation is referred to as 'groups of firms in a particular industry or entire industry sectors that agree to act in prescribed ways, according to a set of rules or principles. Participation by firms in the groups is often voluntary but could also be legally required' (OECD, 2015).

The GSMA, representing the interest of mobile operators worldwide, published *IoT Security Guidelines*. The document was last updated in 2020 and provides an *Overview Document* which is accompanied by *IoT Security Guidelines for IoT Service Ecosystems* and *IoT Security Guidelines for IoT Endpoint Ecosystems* as well as an *IoT Security Assessment Checklist* and *Guidelines for Network Operators* (GSM Association, 2020). It addresses the challenges created by the IoT, presents a risk assessment and gives security recommendations for IoT Service Ecosystems ('services, platforms, protocols, and other technologies required to provide capabilities and collect data from Endpoints deployed in the field') and IoT Endpoint Ecosystems ('low complexity devices, rich devices and gateways that connect the physical world to the digital world') (GSM Association, 2020). The goal of the document set is to encourage the use of IoT security best practices and lessen risks (GSM Association, 2020).

2.4 Enterprise Architecture

EA, according to IEEE, is defined as 'the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.' EA delivers a long-term view approach of a company's required technology and systems (Ross, Weill, & Robertson, 2006). To avoid the existence of uncoordinated and unadaptable legacy systems, the use of architecture is essential in business and IT (Lankhorst, 2013). EA is a tool that provides several perspectives in order to tackle the complexity of an organization. This use can range from a strategic, a tactical or an operational

transformation level. In comparison to EA, a reference architecture is a general architecture that incorporates best-practices and puts the emphasis on the operational view (Greefhorst & Proper, 2011). Benefits of EA are business-related as they enable knowledge management, adaption and the improvement of operations as well as IT-related by reducing complexity and resource management and increasing visibility (Xu, 2015).

2.5 Modelling with ArchiMate

Created by the Open Group, ArchiMate is an open-source tool that can be applied with various functionalities of EA (The Open Group, 2013). It is a modelling language that is used to describe, analyze and visualize the information connected to business processes and IT infrastructure and generate insights for the right stakeholders. The main concepts include a division into business, application, technology and implementation & migration layer as well as a division into passive, behavioral, active and motivational structure (Lankhorst, 2013). ArchiMate finds utilization in modelling various domains and form of analysis: Ranging from Risk Analysis to a SWOT Analysis (Hosiaisluoma, 2019).

The Open Group Architecture Framework (TOGAF) is an EA methodology by the Open Group and is referred to as a 'high level approach for design' (The Opengroup, n.d.). Its primary aim is to ensure consistency and is designed in a modular structure. It can be applied within ArchiMate by combining the respective ArchiMate layer with the according TOGAF phase. This combination as well as a visualization of the ArchiMate structure, the TOGAF standard and relations that can be applied with ArchiMate, are displayed in Appendix E.

3. Research Design

3.1 Methodology

This paper applies the Design Research Methodology (DSRM). The methodology consists of a 'cycle' in which 'IT artifacts' are constructed and assessed (Hevner, March, Park, & Ram, 2004). These IT artifacts can be constructs, models, methods and instantiations. The DSRM consists of six steps that are performed in an iterative approach. In the course of this paper, one

iteration of the cycle is performed consisting of the following steps: **1. Problem Identification and Motivation** that defines the problem and highlights the importance of the problem (see chapter 3.2), **2. Definition of objectives of solution,** that defines what an improved artifact would accomplish (see chapter 4), **3. Design and Development** that creates the artifact (see chapter 5), **4. Demonstration** where the artifact is used to solve the problem (see chapter 6), **5. Evaluation** where the cycle can iterate back to 3. Design (see chapter 7), **6. Communication**, which consists of a professional publication that is found in form of this paper (Pfeffers, Tuunanen, & Chatterjee, 2007-8).

3.2 Research Problem Identification, Research Motivation and Research Question

To better understand the status and perception of IoT security Regulations in various industries, a survey was conducted collecting information from 46 IoT professionals, of which 63 % have already experienced a cyber security attack in their professional context. The most relevant results are presented below, while the full details of the survey can be accessed in Appendix F.

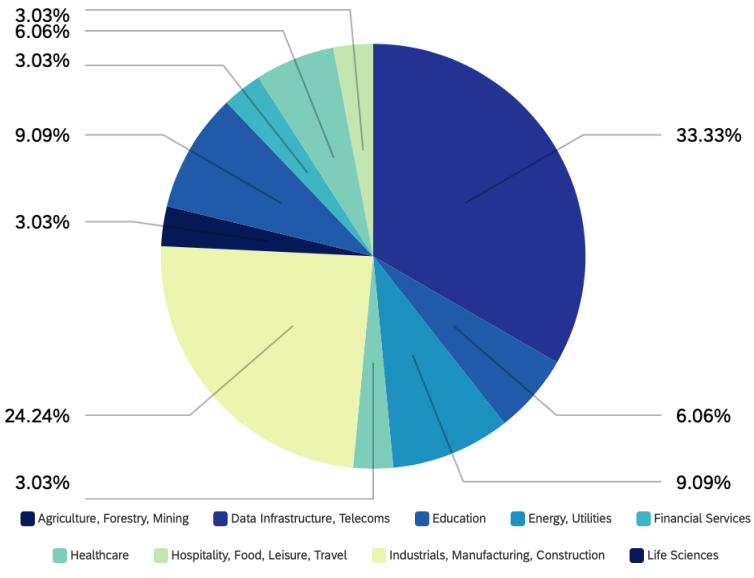


Figure 1: Industry overview of participants in percent

The participants mainly worked in Data Infrastructures/ Telecoms or Industrials Manufacturing and Construction and the majority held the role of either Experts or Managers/Advisors (making up a proportion of 38 % each).

Overall, 83 % of the participants disagreed that current IoT security regulations are clear and up to date (52 % somewhat disagreeing, 31 % disagreeing). 60 % of the participants responded that their company's maturity level is above or somewhat above average. 34 % of the participants answered that mandatory legislations and regulations would help the most to strengthen IoT security, followed by 22 % stating that it would be

regulations according to the own maturity level of the company, when asked to rate what would strengthen IoT security the most. Of the surveyed participants the majority does currently not consult IoT security frameworks (24 %), followed by the most consulted framework: the GMSA framework (22 %):

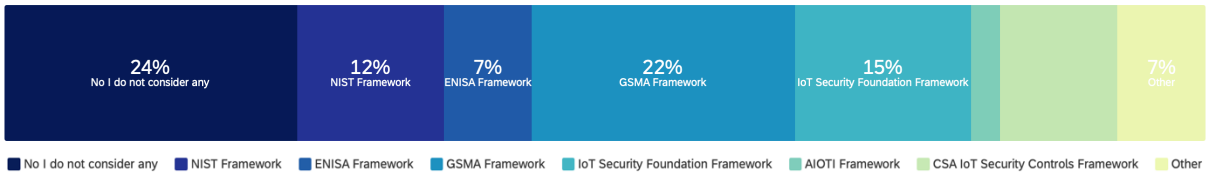


Figure 2: Consulted IoT security frameworks in percent

49 % of the participants state that legislation will probably and 29 % said that it will definitely strengthen IoT security, while 66 % state that regulation will probably strengthen IoT security and 17 % say it will definitely strengthen IoT security. The majority of participants (43 % probably yes, 37 % definitely yes) answered that a common reference architecture will strengthen IoT security. The participants were asked to evaluate eight different IoT security approaches. Frameworks and Standards as well as Security by Design received the highest rate of approval (16 % Agree each). The highest disagreement (60 %) can be found for Security Requirements for IoT Manufacturers.

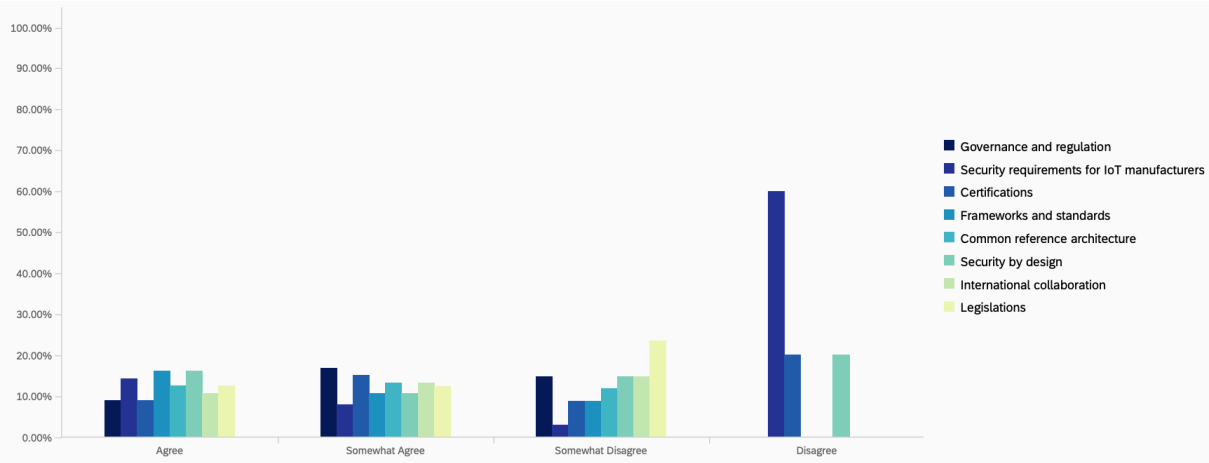


Figure 3: Degree of approval for measures than can foster IoT security in percent

45 % of the participants disagreed that the current IoT security regulations are clear and future proof. 30 % of the participants agreed that legislation will create a safer IoT environment. The majority agreed that a new approach for regulating is needed as same regulation has failed.

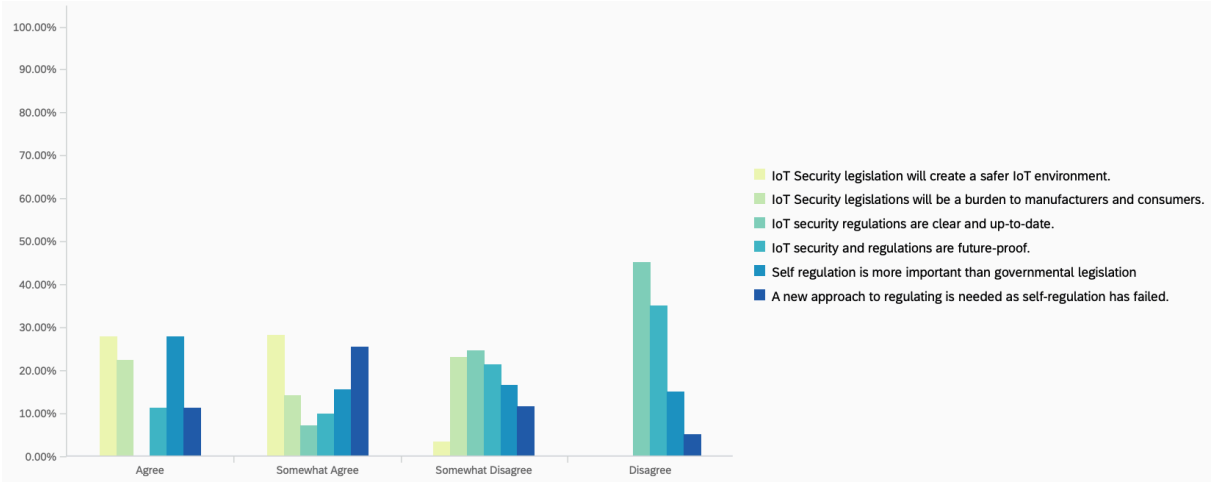


Figure 4: Degree of approval on IoT measures in percent

Chapter 2.1 presented the most critical industries for applications of IoT based on literature review. In contrast to this, according to the surveyed IoT experts, regulations are most necessary for the industries health, energy and banking/ financial services.

For the sake of simplicity, the proportions above were given without naming each appropriate confidence interval. However, it is remarked that the results should be read in the following way: there is a 90 % chance that the real value of those consulting the GSMA framework is within ± 0,1 ME of the surveyed value 22 %. For more details, please refer to Appendix F.

Thus, it becomes visible, that IoT security is an important topic for which the majority of experts agree that more regulatory approaches are needed and that frameworks, standards as well as security requirements for IoT manufacturers are the means to stregthen security. Aiming to combine this with EA, the derived research question is:

RQ: How can IoT Security Regulations be improved using Enterprise Architecture?

4. Definition of Objectives of Solution

To answer the research question, it is proposed to model the two selected IoT security frameworks *Baseline Security Recommendations for IoT (ENISA)* and *IoT Security Guidelines (GSMA)* including the specifications for *IoT Service and Endpoint Ecosystems* using EA with the software Archi. To evaluate and validate the modelled results, Moody and Shanks (2002)

published a framework which allows the validation of models. This framework includes the following qualitay factors:

Correctness: Is the model technically complete? **Completeness:** Does the model cover all user requirements? **Flexibility:** How well can the model be adjusted to business and/or regulatory changes? **Simplicity:** Does the model possess the minimum needed quantity of entitites and relationships? **Integration:** Is the model consistent with the data of the organization? **Understandability:** Are the concepts and the structure of the model understandable? **Implementability:** Can the model be implemented under the time, budget and technological restrictions given? (Moody & Shanks, 2002) These quality factors are mapped to the modelled results in chapter 7.

5. Design and Development

The ArchiMate model consists of top-level folders that represent the applicable layers, relations and views that are summarized in the model tree. The business layer is presented in yellow, the application layer in blue, the technology layer in green and the motivation layer in purple. New views are added to the model tree and allow a classification of perspectives as well as drilling down for specific details (The Open Group, 2013). An overview of applicable relations in ArchiMate are listed in Appendix E.

In the first step, a metamodel was created in ArchiMate. A metamodel is defined as a ‘minimum set of architectural content to support traceability across artifacts’ (The Opengroup, n.d.) and functions as an overall reference to better understand the modelling structure. The overall metamodel is presented below containing the business, application, technology and motivation layer in Figure 5. Afterwards, relevant viewpoints were defined in accordance with the components of the frameworks and the respective metamodels were created for the following viewpoints: Guideline Structure, Motivation, IoT Model, Risk and Threat Analysis, Recommendations and Use Cases.

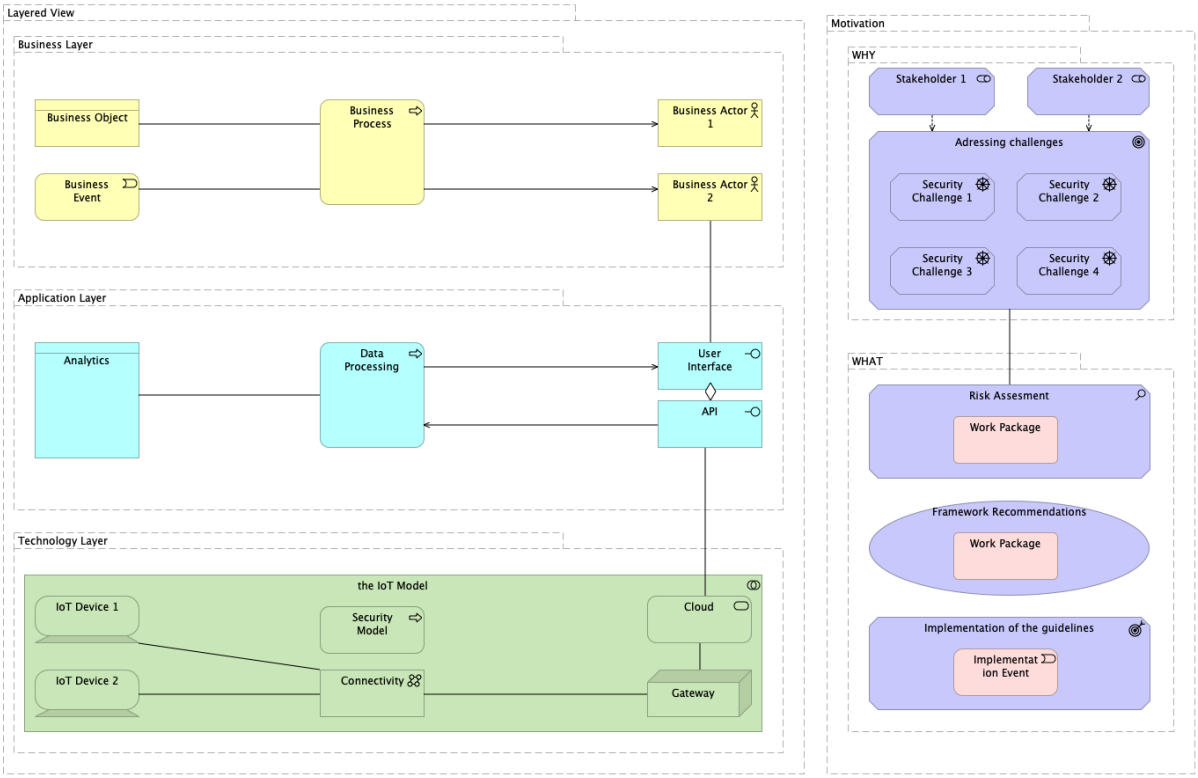


Figure 5: Viewpoint Metamodel

As an example, the metamodel for the motivation viewpoint and the metamodel for the risk assessment/ security model viewpoint is presented. Figure 6 shows the modelled stakeholder elements influencing the overall goal to address challenges. The goal, in turn, is driven by various security challenges. Figure 7 visualizes the metamodel for the risk and threat analysis: Various technology events which represent cyber security attack scenarios on IoT, realize an outcome: The outcome of a cyber security attack impacts the IoT ecosystem with a threat:

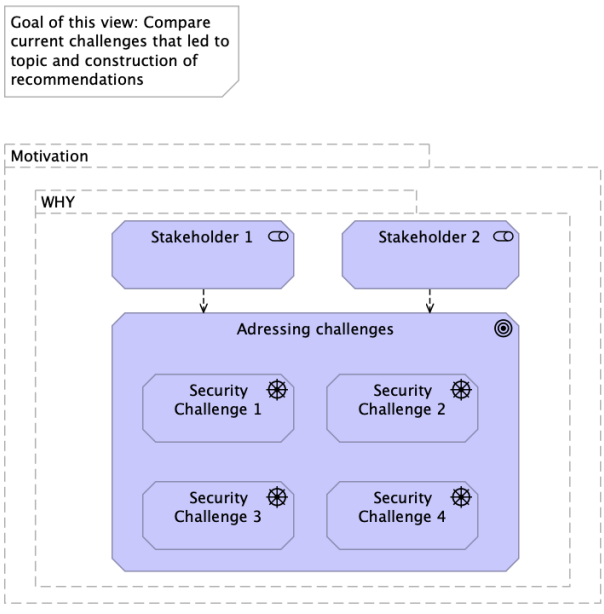


Figure 6: Viewpoint Metamodel Motivation

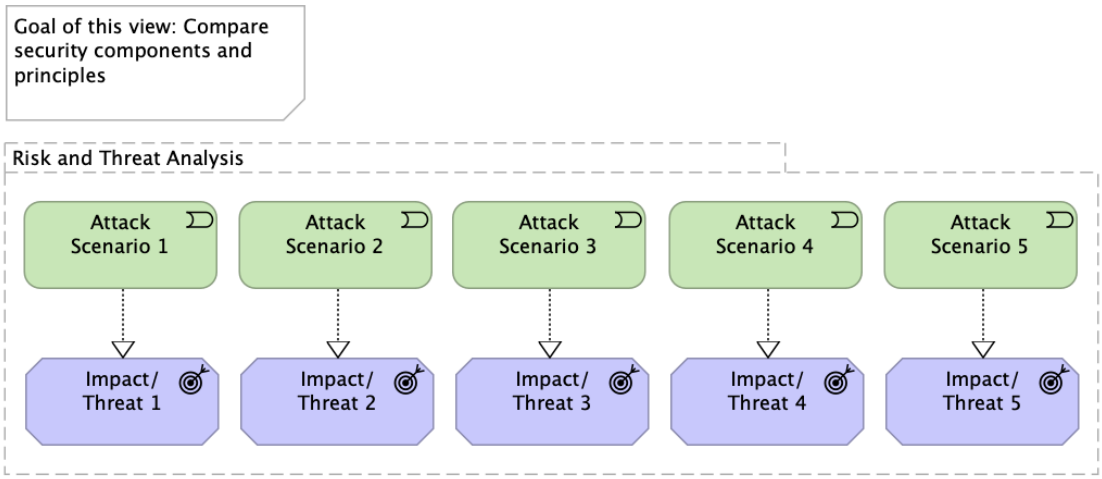


Figure 7: Viewpoint Metamodel Risk and Threat Analysis

Finally, the constructed metamodels for the various viewpoints were filled with the relevant information given by the two consulted IoT security Frameworks. Below, figure 8 displays the model for the motivation viewpoint as well as the model risk and threat analysis viewpoint is for the ENISA and the GSMA framework:

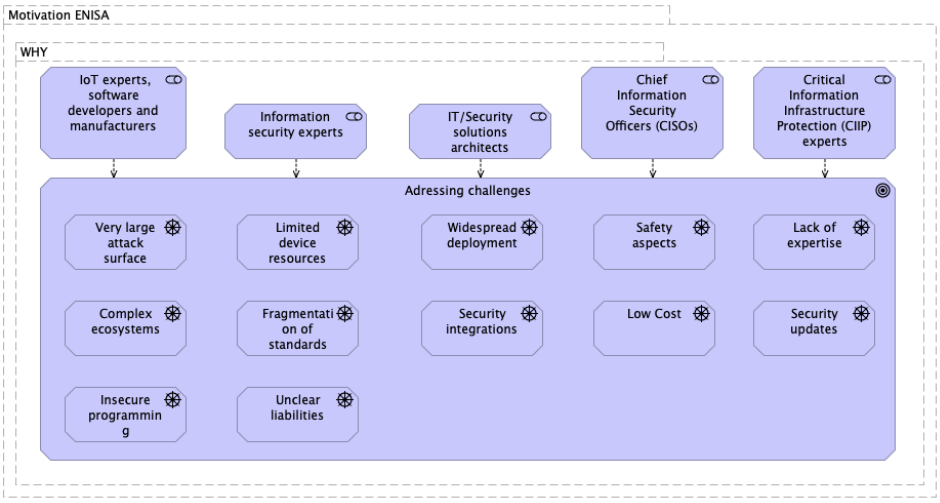


Figure 8: Viewpoint Motivation ENISA

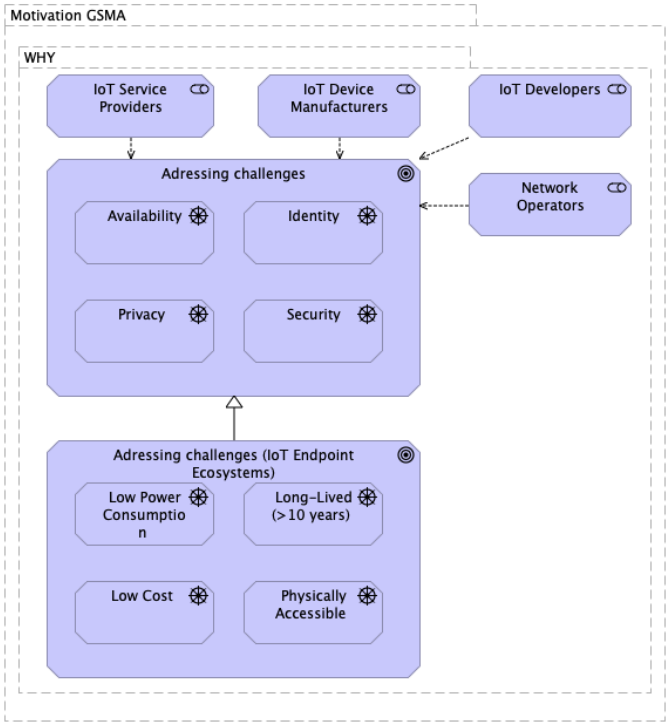


Figure 9: Viewpoint Motivation GSMA

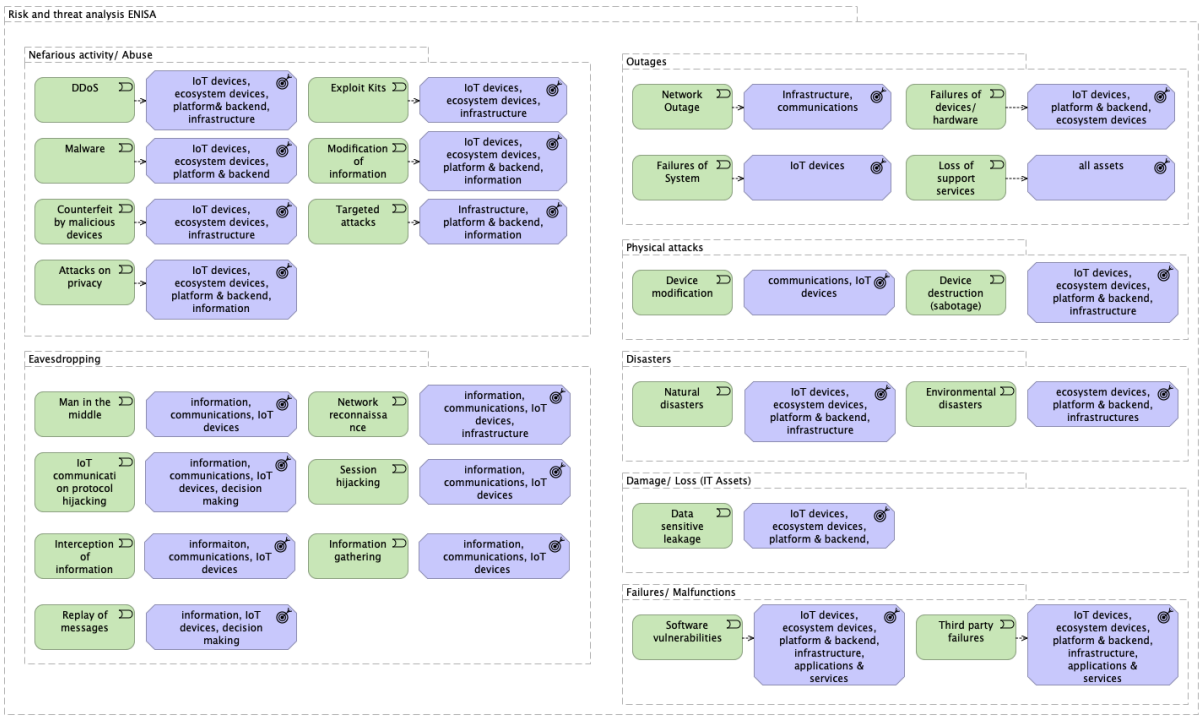


Figure 10:Viewpoint Threat and Risk Analysis ENISA

It becomes visible that the architecture for the same viewpoint varies for each modelled framework: While both include attack scenarios, the threat and risk analysis for ENISA displays the impact on the respective components of the IoT ecosystem for each technology event. The

model for GSMA does not contain specific information on the impact/threat but highlights the differentiation of attack scenarios for IoT service and IoT endpoint ecosystems. A detailed comparison can be found in the next chapter. The remaining viewpoints and models are presented in Appendix G.

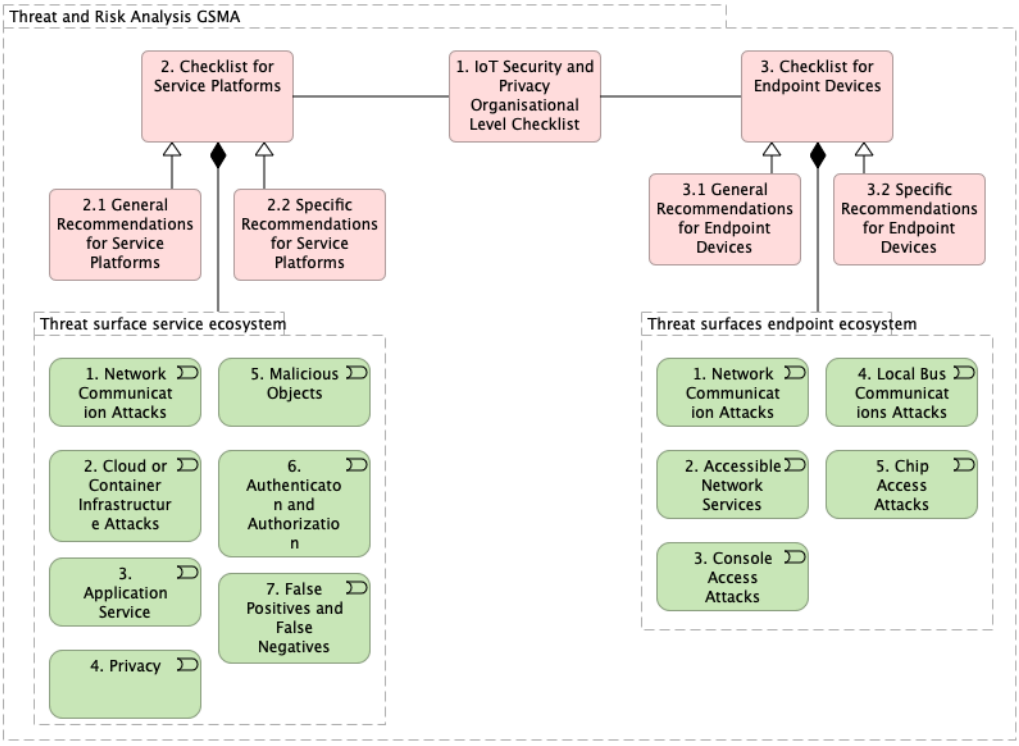


Figure 11: Viewpoint Threat and Risk Analysis GSMA

6. Demonstration

With the help of ArchiMate, the constructed models were analyzed. The results allow a comparison between the frameworks, which is listed in the table below.

The first column refers to the modelled viewpoint. If a specific component of the viewpoint is compared, this component is also specified in that column. The second column displays the overlap of elements that are represented by both frameworks. In the third column the focus of ENISA's document is displaying elements that the ENISA framework proposes and are not present in GSMA's *IoT Security Guidelines*. The fourth column presents the opposite: Elements are displayed that have not been included in the *Baseline Security Recommendations for IoT* by ENISA but are discussed by the GSMA framework.

Table 2: Comparison of Frameworks

View	Intersection	Focus ENISA	Focus GSMA
Guideline Structure View	Specifications for certain verticals, threat analysis, recommendations	Standards Gap Analysis	Differentiation between Service and Endpoint Ecosystems
Motivation View: Stakeholders	IoT Developers, IoT Manufacturers	Information Security Experts, IT/Security solution architects, Chief Information Security Officer	Network Operators, IoT Service Providers
Motivation View: Challenges	Low Cost, safety aspects/ privacy/ security (integrations, updates), large attack surface/ physically accessible	Lack of expertise, complex ecosystems, insecure programming, limited device resources, fragmentation of standards, unclear liabilities, widespread deployment	Availability, identity, low power consumption, long-lived
IoT Model View: Components	communication network, ecosystem	Decision making, information, application services, infrastructure	Partner API, user experience, ecosystem approach
Risk and Threat Analysis View: Structure	List of threats and attack surfaces	Depiction of assets involved in attack scenario/ outcome, grouping of attack types	Detailed description of attack scenarios
Risk and Threat Analysis View: Content	(Attacks on) Privacy, network communication attacks / eavesdropping/ interception/ hijacking (Man in the middle, IoT communication protocol hijacking, interception of information, network reconnaissance,	Nefarious Activity/ Abuse (DDoS, Malware, Exploit Kits, Counterfeit, Targeted Attacks, Modification of information), Outages (failures of devices/hardware, failure of systems, network outages, loss of support services),	Cloud/ container infrastructure attacks, application service, authentication and authorization, false positives and negatives, accessible network services, console access attacks, local bus

	information gathering, session hijacking, replay of messages), malicious objects	physical attacks (device modification, device destruction), disasters (natural disasters, environmental disasters), damage/loss (data sensitive leakage), failure/ malfunctions (software vulnerabilities, third party failures)	communication attacks, chip access attacks
Recommendations View: Structure	Recommendations	Gap analysis, general recommendations for certain stakeholder groups, categorization by policies, organization, people, process and technological measures	Differentiation between critical, high priority, medium priority and low priority recommendations, differentiation between service and endpoint ecosystems
Use Case View: Content	Depiction of exemplary attack scenarios via use cases	IoT administration system compromise, value manipulation in IoT devices, Botnet/commands injection	Wearable heart rate monitor, personal drone, vehicle sensor network

7. Evaluation

To validate the models and the frameworks they are based on, an evaluation is conducted using the quality factors from the Moody and Shanks framework. These factors were elaborated in chapter 4. The Moody and Shanks framework primarily targets the evaluation of data quality models. In this context, it is applied to the created ArchiMate models as well as to the underlying IoT security frameworks:

Correctness: To evaluate whether the model is technically complete, it can be remarked that the IoT model itself as well as the given security threats and the derived recommendations differ between the two modelled frameworks. Thus, this discrepancy was transferred to the respective models. Simultaneously, it should be mentioned that as technology evolves rapidly, it is impossible for an IoT security Framework to be completely up to date and technically complete. Instead, the primal objective of an IoT security framework should be the holistic view of the whole ecosystem. This requirement is fulfilled by the presentation of the IoT model in each framework which has been transferred accordingly into the ArchiMate language.

Completeness: The user requirements of the two modelled frameworks differ as they address different stakeholder groups. While both frameworks aim to address IoT Developers and IoT Manufacturers, the GSMA targets primarily technical stakeholders while ENISA targets strategic users. This is underlined by the varying challenges that are addressed by each framework. It can be stated that the derived IoT challenges for each framework were modelled in accordance to the stakeholders involved and thus the two frameworks and the ArchiMate models cover the relevant user requirements.

Flexibility: The flexibility of both models can be confirmed as viewpoints can be added or adjusted accordingly. For the underlying framework, it is of importance that these are reviewed on a continuous basis. As stated above, ENISA regulary publishes new studies on IoT security and vertical applications that refer to the orgininal study. The GSMA framework was last adjusted in 2020 to incorporate the latest changes. Thus, the frameworks and the models can be categorized as flexible and it is recommended to adjust viewpoints on a regular basis.

Simplicity: It can be confirmed that the proposed models include the minimum needed number of entities and relationships as these are based on the content of the framework. In order to reduce complexity, various viewpoints were implemented to show only the relevant

information to the right stakeholder group. Futhermore, coherent content was grouped and detailed information was displayed in the documentation of the respective elements.

Integration: The model conforms to the model of the organization if the organization itself makes use of explicit and holistic EA. The actual degree of success of integration will, however, only be able to be evaluated upon publication of this paper and after the proposed concept is put into practice and tested in an organization. Feedback on the realization should be used to improve the model and the respective framework in form of an evolution process.

Understandability: The understandability of the modelled frameworks combines two factors: A basic knowledge of technical terms in the context of IoT Security as well as a general understanding of the ArchiMate modelling language and EA concepts. If these two prerequisites are met, the model is understandable as the elements and relations of the model can be interpreted accordingly. Expertise on security is necessary to classify the proposed security measures with the corresponding status quo of an organization.

Implementability: Both frameworks do not provide sufficient information on the implementation of the frameworks. While the GSMA framework provides a detailed security assessment, the follow up and implementation of the analysis is vague. ENISA proposes detailed security recommendations and distinguishes between policy, organizational and technological measures, but misses out on linking these with practicability. This is reflected in the models: An implementation viewpoint for each model is missing. It is recommended to give further advice as for the implementations of security measures and the maintenance of technological updates which then are added to complement the models.

Overall, the Moody and Shanks framework strengthens the need for stronger implementation and integration measures. Practicability and adaptability are of great importance in a setting of rapid technological development that can be found with IoT technology.

8. Conclusion and Limitations

The increasing importance of security for the IoT is depicted: Ranging from a literature review on the characteristics of the technology and its security threats to a survey of IoT experts, the paper underlines that the relevance of IoT security is high. The study focuses on regulatory approaches to which industry experts responded to in favor of stronger measures and more transparency: 45 % agreed that the current status is not clear and up to date. This can also be concluded from the overview of current IoT security approaches presented in chapter 2.3. Furthermore, the survey highlighted a stronger use of operational IoT security frameworks in comparison to strategic frameworks like those of ENISA, suggesting a governance issue.

Two selected IoT security frameworks *Baseline Security Recommendations for IoT* by ENISA and *IoT Security Guidelines* by the GSMA show the applicability of EA in this context: Visualization with the EA modelling language ArchiMate highlights attack surfaces in the IoT ecosystem, models use cases and presents security recommendations in a structured way. Moreover, it facilitates the comparison between security frameworks. The evaluation of the model's quality factors with the help of the Moody and Shanks framework underlines the fulfillment of the factors **flexibility**, **simplicity** and **understandability**. Furthermore, technological development is needed for the quality factor **correctness** while the factor **completeness** is dependent on the targeted stakeholder group. It is proposed that the factors **integration** and **implementability** are tested in a next step in order to validate the model in an organization. Overall, the answer to the RQ: 'How can IoT Security Regulations be improved using Enterprise Architecture?' is: EA is a meaningful tool to visualize, analyze and compare IoT security frameworks. This is an essential step and advantage due to the great supply of existing IoT security approaches that are not fully coherent, complete, up to date and published by a wide range of organizations. Owing to its layered approach that integrates various viewpoints and relations, EA can strengthen the understandability of an IoT security

framework: Flexible viewpoints present relevant information to the appropriate stakeholder group, use cases are visualized as references for best practices and a common understanding is created with the help of metamodels and reference architectures. In addition, EA provides a tool to assist finding the suitable framework to meet the needs of an organization. Especially, the visualization of attack surfaces in an IoT ecosystem is of great relevance as security is determined by the weakest component in an IoT technology stack. As depicted in chapter 2.4, EA enables business and IT related advantages: By using EA for IoT security frameworks, knowledge management on IoT security measures and recommendations increase. This reflects on the operations of an organization. The use of EA reduces complexity and resource management as critical scenarios and vulnerable attack surfaces are mapped out.

However, the paper also contains limitations: Firstly, as the supply of IoT security approaches is large, continuously evolving and influenced by a variety of organizations, the modelling of the two selected approaches is exemplary. Using EA to model more IoT security frameworks in a larger sample is recommended to validate the usability of EA for IoT security regulation and especially for IoT security frameworks Also, the above analysis has been built on the argument of displaying one framework from a regulatory agency and one from a self-regulatory organization. Here, the view of comparison may differ. Furthermore, for geographical regions, different IoT security frameworks may be of interest. In this paper, two frameworks have been chosen that have an impact on the European Union. ENISA, for instance, may only be relevant for the European market. Further limitations regarding the conducted survey in chapter 3.1 are the provided sample size, containing 46 participants, as well as the structure of the survey. Results must be interpreted with the respective confidence interval and it must be considered that not all participants responded to all questions due to the specificity of the topic. In course of this paper, the surveyed results are used to support the relevance of the topic and the research motivation and are not intended to reject or accept a given hypothesis.

9. Directions for Future Research

The paper proposes the following directions for future research: As 43 % of the surveyed participants stated that a common IoT security reference would strengthen IoT security, a common reference architecture modelled in EA for IoT security is suggested. Moreover, it is recommended to specify a IoT security reference architecture for specific industries or vertical applications. For instance, a common IoT security reference architecture for critical infrastructures in the energy sector may highlight relevant attack surfaces and derive security measures. IoT security frameworks are not a one fits all solution and the more the recommendations are adjusted to the analyzed sector, the better. This application is especially important for the health or financial services sector and for essential services in general.

Secondly, new standards and technological components are permanently under development: it is proposed to ensure the regular revision of technological updates and their respective security measures within a IoT security framework. The update must then be transferred to the EA model. Further analysis of implementation and integration of EA models should be considered: Not only for an organization implementing a new IoT security framework, but also for international collaboration. EA presents the possibility to facilitate cooperation on common IoT security measures and visualize gaps and overlaps. It may also be interesting to examine how evolving technologies like blockchain, fog computing, machine learning and edge computing will impact IoT security in terms of EA. EA can be used to model the intersection of these technological opportunities and their potentials improved security for the IoT.

To further validate the surveyed results, tools like the Principal Components Analysis can be used that allow the identification of underlying components. Also, increasing the sample size will result in an increase of the relevance of the survey results.

Finally, the applied DRSM methodology proposes research in cycles. The next steps should be implemented in an iterative approach considering the proposed improvements for the model and directions for further research.

References

Acohido, B. (2020, November 6). *IoT Attacks Intensified by Covid-19*. Retrieved December, 2020 from www.securityboulevard.com: https://securityboulevard.com/2020/11/iot-attacks-intensified-by-covid-19-avast/

AD for Policy and Strategy. (n.d.). *Definition of policy*. Retrieved December 2020, from www.cdc.gov: https://www.cdc.gov/policy/analysis/process/definition.html

Cambridge dictionary. (n.d.). *Governance*. Retrieved December 2020, from www.dictionary.cambridge.org: https://dictionary.cambridge.org/dictionary/english/governance

Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cyberseucirty policies and use cases in U.S. federal government. *Government Information Quarterly*, 346-357.

Christou, G. (2018). The challenges of cybercrime governance in the European Union. *European Politics and Society, 19:3*, 355 - 375, DOI: 10.1080/23745118.2018.1430722.

Cloud Security Alliance. (2019, May 03). *CSA IoT Security Controls Framework.* From www.cloudsecurityalliance.org: https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/

Das, A. K., Kumar, N., & Srinivas, J. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Comupter Systems*, 178-188.

Dhanjani, N. (2015). *Abusing the Internet of Things. Blackouts, Freakouts, and Stakeouts.* Sebastopol, CA: O'Reilly Media, Inc.

ENISA. (2017, November 20). *Baseline Security Recommendations for IoT.* From www.enisa.europa.eu: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

ENISA. (2019, January 17). *IoT Security Standards Gap Analysis.* From www.enisa.europa.eu: https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis

ENISA. (2019, June 26). *The European Union Agency for Cybersecurity - A new chapter for ENISA.* Retrieved December, 2020 from www.enisa.europa.eu: https://www.enisa.europa.eu/news/enisa-news/the-european-union-agency-for-cybersecurity-a-new-chapter-for-enisa

ENISA. (2019, November 19). *www.enisa.europa.eu.* From Good Practices for Security of IoT - Secure Software Development Lifecycle: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

ENISA. (2020, November 09). *Guidelines for Securing the Internet of Things.* From www.enisa.europa.eu: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

ENISA. (n.d.). *EU cybersecurity certification framework*. Retrieved December 2020, from www.enisa.europs.eu: https://www.enisa.europa.eu/topics/standards/certification

Eugen, P., & Petrut, D. (2018). Exploring the New Era of Cybersecurity Governance. *"Ovidius" University Annals, Economic Sciences Series Volume XVIII, Issue 1 /2018*, 358 - 363.

Gartner. (n.d.). *Standards*. Retrieved December 2020, from www.gartner.com: https://www.gartner.com/en/information-technology/glossary/standards

Glen, S. (n.d.). *Margin of Error: Defintion, How to Calculate in Easy Steps*. Retrieved December 2020, from statisticshowto.com: https://www.statisticshowto.com/probability-and-statistics/hypothesis-testing/margin-of-error/

Greefhorst, D., & Proper, E. (2011). *Architecture Principles. The Cornerstones of Enterprise Architecture.* Berlin Heidelberg: Springer.

GSM Association. (2020, February 29). *IoT Security Guidelines for Service Ecosystems.* From www.gsma.com: https://www.gsma.com/iot/iot-security-guidelines-for-iot-service-ecosystem/

GSM Association. (2020, February 29). *IoT Security Guidelines for Endpoint Ecosystems.* From www.gsma.com: https://www.gsma.com/iot/iot-security-guidelines-for-endpoint-ecosystem/

GSM Association. (2020, February 29). *IoT Security Guidelines Overview Document.* From www.gsma.com: https://www.gsma.com/iot/iot-security-guidelines-overview-document/

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access*.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 75-106.

Hewlett Packard. (n.d.). *What is a reference architecture?* Retrieved December 2020, from www.hpe.com: https://www.hpe.com/us/en/what-is/reference-architecture.html

Hosiaisluoma, E. (2019). *ArchiMate Cookbook. Patterns & Examples.* From www.hosiaisluoma.fi: http://www.hosiaisluoma.fi/ArchiMate-Cookbook.pdf

IEEE Internet of Things. (n.d.). Retrieved December 2020, from www.standards.ieee.org: https://standards.ieee.org/initiatives/iot/index.html

IEEE. (n.d.). *IEEE 1471-2000 - IEEE Recommended Practice for Architectural Description for Software-Intensive Systems*. Retrieved December 2020, from www.standards.ieee.org: https://standards.ieee.org/standard/1471-2000.html

IoT Alliance Australia. (n.d.). *Resources and Publications*. Retrieved December 2020, from www.iot.org.au: https://iot.org.au/resources/

IoT Security Foundation. (n.d.). *IoT Security Foundation Publications*. Retrieved December 2020, from www.iotsecurityfoundation.org: https://www.iotsecurityfoundation.org/best-practice-guidelines/

ISO. (n.d.). *ISO Standards*. Retrieved December 2020, from www.iso.org: https://www.iso.org/standards.html

Khodadadi, F., Dastjerdi, A., & Buyya, R. (2016). Chapter 1: Internet of Things: An Overview. In R. Buyya, & A. V. Dastjerdi, *Internet of Things. Principles and Paradigms* (pp. 3-23). Cambridge, MA: Elsevier Inc.

Lankhorst, M. (2013). *Enterprise Architecture at Work. Modelling, Communication and Analysis (3rd ed.).* Berlin Heidelberg: Springer.

Lee, G. (2019). What roles should the government play in fostering the advancement of the internet of things? *Telecommunications Policy*, 434-444.

Lueth, K. L. (2020, November 19). *iot-analytics.com*. Retrieved November 19, 2020 from https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

Merriam-Webster. (n.d.). *Best practice*. Retrieved December 2020, from www.merriam-webster.com: https://www.merriam-webster.com/dictionary/best%20practice

Mirriam-Webster. (n.d.). *Defintion of legislation*. Retrieved December 2020, from www.merriam-webster.com: https://www.merriam-webster.com/dictionary/legislation

Moody, D. L., & Shanks, G. G. (2002). Improving the quality of data models: empirical validation of a quality management framework. *Information Systems*.

NIST. (n.d.). *NIST Cybersecurity for IoT Program*. Retrieved December 2020, from www.nist.gov: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

O'Donnell, L. (2019, June 27). *Thousands of IoT Devices Bricked By Silex Malware*. Retrieved December, 2020 from www.threatpost.com: https://threatpost.com/thousands-of-iot-devices-bricked-by-silex-malware/146065/

OECD. (2002, January 3). *Regulation* . From www.stats.oecd.org: https://stats.oecd.org/glossary/detail.asp?ID=3295

OECD. (2015, March 23). *Industry-self-regulation: Role and use in supporting consumer interests.* From www.oecd.org : https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2014)4/FINAL&docLanguage=En

Pfeffers, K., Tuunanen, T., & Chatterjee, S. (2007-8). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 45-78.

Pipelinesecurity. (2020, May 20). *The Internet of Things (IoT) and the Consequences of Cyber Attacks*. Retrieved December 2020, from www.pipelinesecurity.net: https://www.pipelinesecurity.net/the-internet-of-things-and-the-consequences-of-cyber-attacks/

Polverini, D., Ardente, F., Sanchez, I., Mathieux, F., Tecchio, P., & Beslay, L. (2018). Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process. *Computer & Security*, 295-310.

Rabeau, A. (n.d.). *Regulatory Frameworks*. Retrieved December 2020, from www.qp.gov.bc: http://www.qp.gov.bc.ca/rcwc/research/intersol-frameworks.pdf

Rosner, G. (2017). *Privacy and the Internet of Things.* Sebastopol, CA: O'Reilly Media, Inc.

Ross, J. W., Weill, P., & Robertson, D. C. (2006). *Enterprise Architecture as Strategy. Creating a Foundation for Business Execution.* Boston, MA: Harvard Business Press.

Slama, D., Puhlmann, F., Morrish, J., & Bhatnagar, R. M. (2016). *Enterprise IoT.* Sebastopol, CA: O'Reilly Media, Inc.

Techslang. (n.d.). *Security Framework.* Retrieved December 2020, from www.techslang.com: https://www.techslang.com/definition/what-is-a-security-framework/

The Open Group. (2013). *Archi. User Guide.* From www.archimatetool.com: https://www.archimatetool.com/downloads/Archi%20User%20Guide.pdf

The Opengroup. (n.d.). *Content Metamodel*. Retrieved December 2020, from www.opengroup.org: https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap30.html

The Opengroup. (n.d.). *the TOGAF Framework*. Retrieved December 2020, from www.opengroup.org: https://pubs.opengroup.org/architecture/archimate3-doc/apdxd.html

Urgessa, W. G. (2019). Multilateral cybersecurity governance: Divergent conceptualizations and its origin. *Computer Law & Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j. clsr.2019.105368*.

von Solms, B., & von Solms, R. (2018). Cybersecurtiy and information security - what goes where? *Information and Computer Security*, 2-9.

Xu, L. D. (2015). Chapter 4: Enterprise and Supply Chain Architecture. In L. D. Xu, *Enterprise Integration and Information Architecture. A Systems Perspective on Industrial Information Integration* (pp. 129-136). Taylor & Francis Group.

Appendix

A. List of Figures

B. List of Tables

C. List of acronyms

D. Definitions and terms

E. ArchiMate and TOGAF

F. Survey

G. ArchiMate Models

A. List of Figures

B. List of Tables

C. List of acronyms

CIA – Confidentiality, Integrity, Availability
DDoS - Distributed Denial-of-service
EA – Enterprise Architecture
ENISA - European Network and Information Security Agency
GSMA – Global System for Mobile Communications Association
IoT – Internet of Things
OECD - Organisation for Economic Co-operation and Development
SWOT -Strengths, Weaknesses, Opportunities, Threats
TOGAF - The Open Group Architecture Framework

D. Definitions and terms

(Cyber security) Certification – According to ENISA, Certifications are defined as 'the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria, standards, and the issuing of a certificate indicating conformance; as such cybersecurity certification plays a key role in increasing trust and security in products, services and processes.'

(Security) Framework – Defined by Techslang as 'a compilation of state-mandated and international cybersecurity policies and processes to protect critical infrastructure. It includes precise instructions for companies to handle the personal information stored in systems to ensure their decreased vulnerability to security-related risks.'

Best Practices – According to Merriam-Webster 'a procedure that has been shown by research and experience to produce optimal results and that is established or proposed as a standard suitable for widespread adoption.'

Governance – Defined by Cambridge Dictionary as 'the way that organizations or countries are managed at the highest level, and the systems for doing this.'

Legislation – 'The exercise of the power and function of making rules (such as laws) that have the force of authority by virtue of their promulgation by an official organ of a state or other organization' (Mirriam-Webster, n.d.).

Policy – 'A law, regulation, procedure, administrative action, incentive, or voluntary practice of governments and other institutions. Policy decisions are frequently reflected in resource allocations' (AD for Policy and Strategy, n.d.).

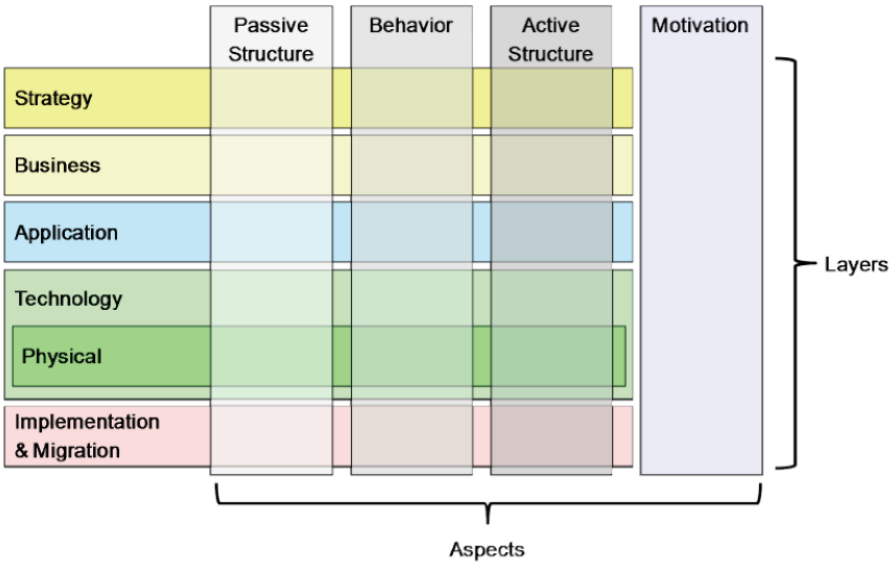
Reference Architecture – 'A document that provides recommended structures and integrations of IT products and services to form a solution. It includes accepted industry best practices, typically suggesting the optimal delivery method for specific technologies' (Hewlett Packard, n.d.).

Regulation - Regulation can be defined as the 'imposition of rules by government, backed by the use of penalties that are intended specifically to modify the economic behavior of individuals and firms in the private sector' (OECD, 2002).

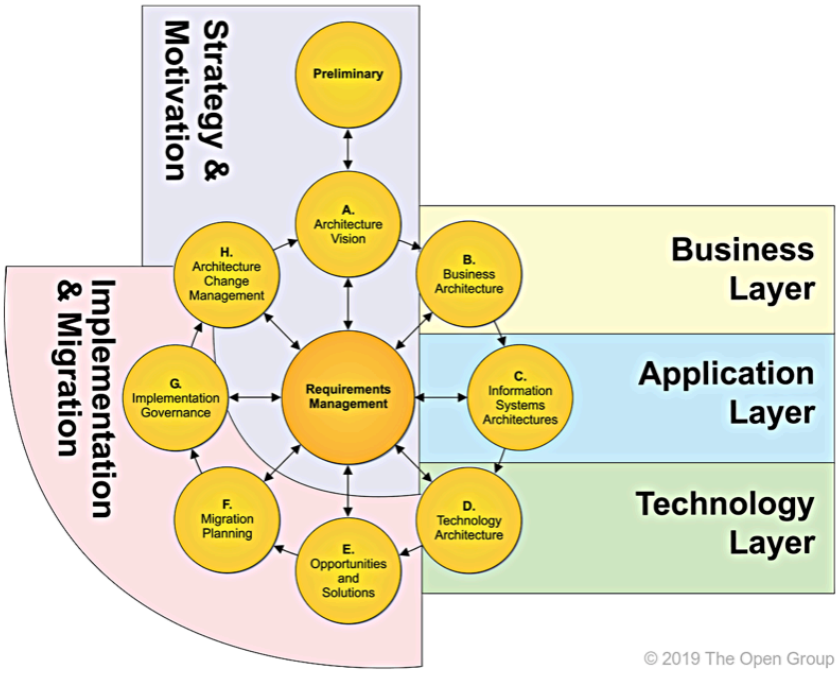
Self-regulation - Industry-self-regulation can be referred to 'groups of firms in a particular industry or entire industry sectors that agree to act in prescribed ways, according to a set of rules or principles. Participation by firms in the groups is often voluntary but could also be legally required' (OECD, 2015).

Standards – 'Specifications or styles that are widely accepted by users and adopted by several vendors. Standards are critical to the compatibility of hardware, software, and everything in between. Industry standards enable the essential elements of a computer and related infrastructure to work together' according to Gartner.

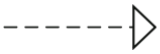
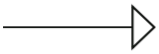
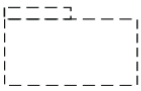
E. ArchiMate and TOGAF



Aspects and Layers in ArchiMate Core Framework. Source: (Hosiaisluoma, 2019)



Correspondence between ArchiMate and TOGAF. Source: (The Opengroup, n.d.)

Association	*Association* models a relation between objects that is not covered by another, more specific relationship.
Access 	The *access* relation models the access of behavioural concepts to business or data objects.
Used by 	The *used by* relation models the use of services by processes, functions, or interactions and the access to interfaces by roles, components, or collaborations.
Realisation 	The *realisation* relation links a logical entity with a more concrete entity that realises it.
Specialisation 	The *specialisation* relation indicates that an object is a specialisation of another object.
Assignment	The *assignment* relation links units of behaviour with active elements (e.g., roles, components) that perform them, roles with actors that fulfil them, or artifacts that are deployed on nodes.
Aggregation 	The *aggregation* relation indicates that an object groups a number of other objects.
Composition 	The *composition* relation indicates that an object consists of a number of other objects.
Grouping 	The *grouping* relation indicates that objects belong together based on some common characteristic.

Relations in Enterprise Architecture. Source: (Lankhorst, 2013)

F. Survey

Remarks concerning the survey:

The survey was conducted from 12.11.2020 until 06.12.2020 and distributed via LinkedIn. Participants where not obliged to answer every question in order to avoid random guessing. Thus, the number of responses for each question may vary.

Example calculation to compute the confidence interval for a proportion:

The sample size is equal to n = 46. It was decided to use a confidence level of 90 %. As we do not know whether we have a normal distribution but possess a sample of size of 46 that is > 30, we can use the Z-Score. The Z-Score for a 90 % confidence level is equal to 1.645. The margin of error for a proportion is calculated ME = $Z * \sqrt{\frac{p-hat\ (1-p\ hat)}{n}}$ with p-hat representing the sample proportion. Our confidence interval can then be calculated for our sample proportion, $\hat{p}$: CI, $\hat{p}$, 90% = [$\hat{p}$ + ME; $\hat{p}$ - ME], thus there is a 90 % chance that the real value is within ± ME of the measured value (Glen, n.d.).

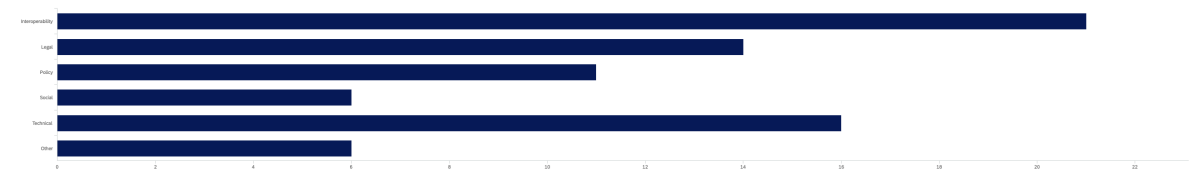
Example: There is a 90 % chance that the real value of those consulting the GSMA framework is within ± 0,10 ME of the surveyed value 22 %.

Questions and results of survey:

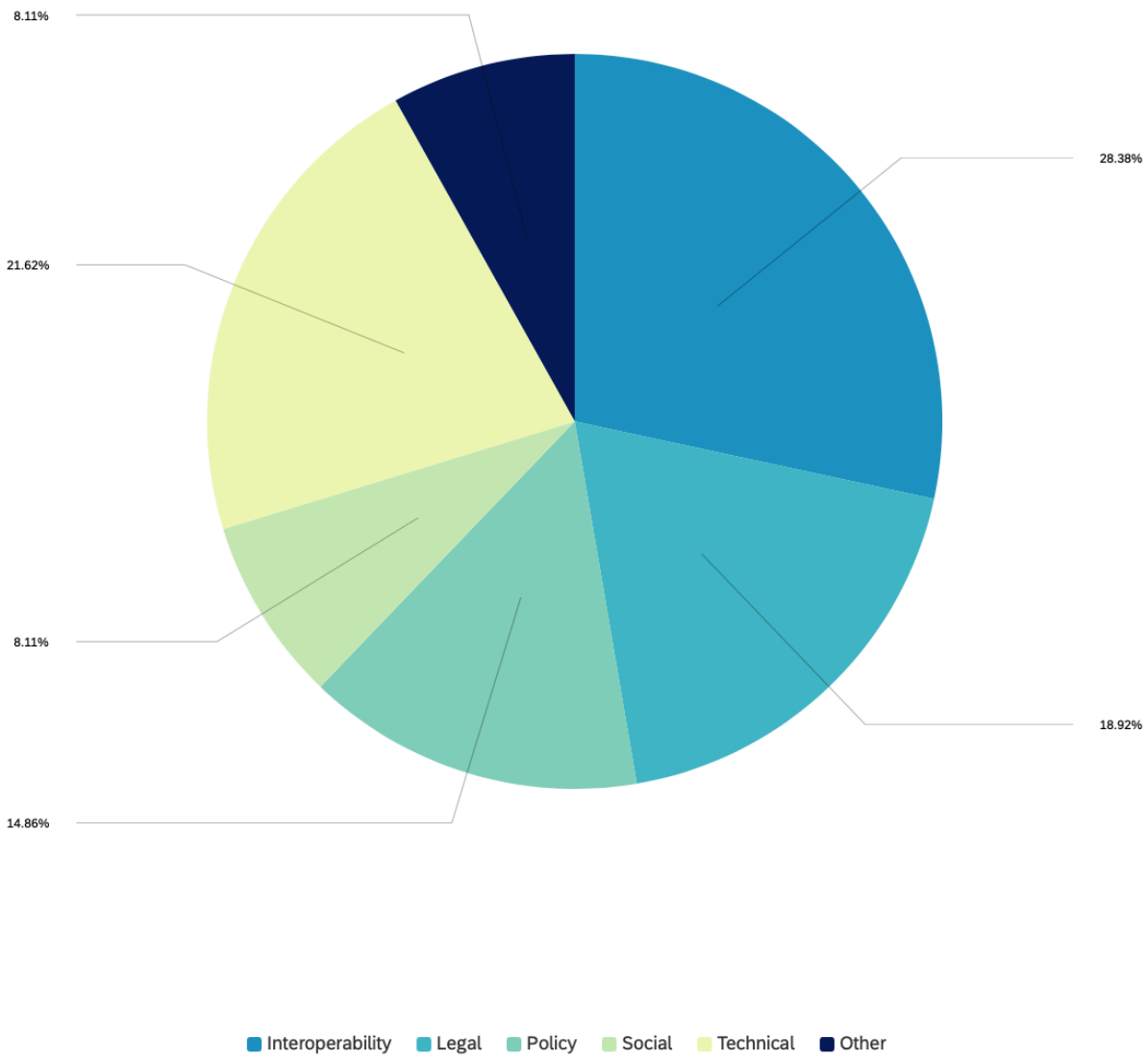
1) Where do you see the biggest challenges for the IoT?

Q1 - Where do you see the biggest IoT challenges? Select all that apply.

Page Options



#	Field	Choice Count
1	Interoperability	28.38% 21
2	Legal	18.92% 14
3	Policy	14.86% 11
4	Social	8.11% 6
5	Technical	21.62% 16
6	Other	8.11% 6
		74



2) Will legislation strengthen IoT security?

Q2 - Will legislation strengthen IoT security? Select one.

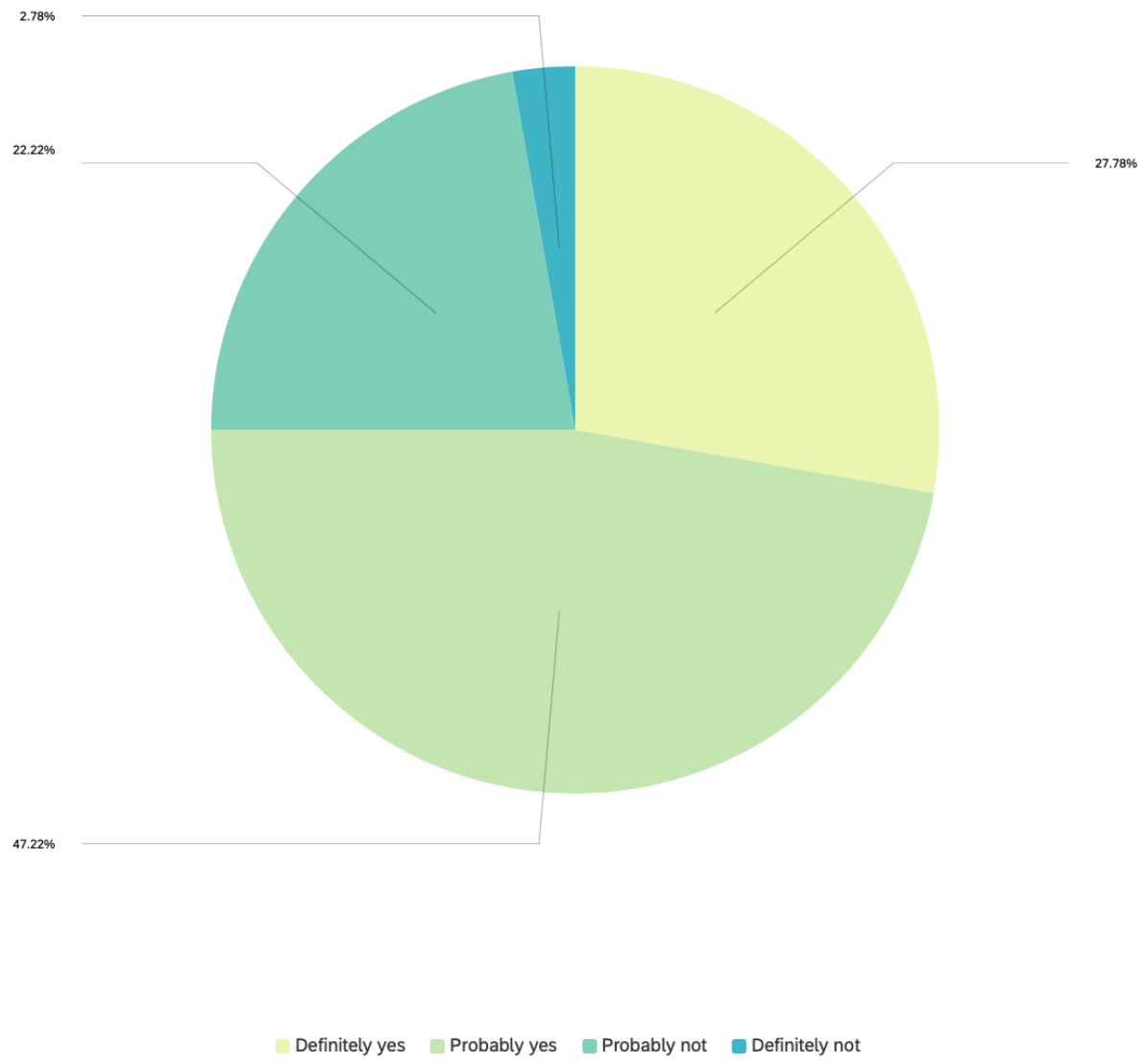
Page Options

Retrieving data...

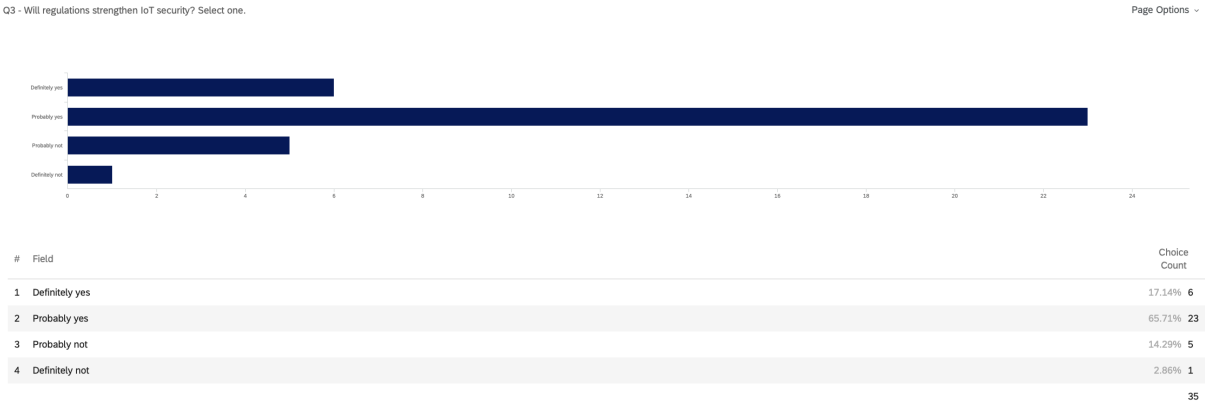
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Will legislation strengthen IoT security? Select one.	1.00	4.00	2.00	0.78	0.61	36

Retrieving data...

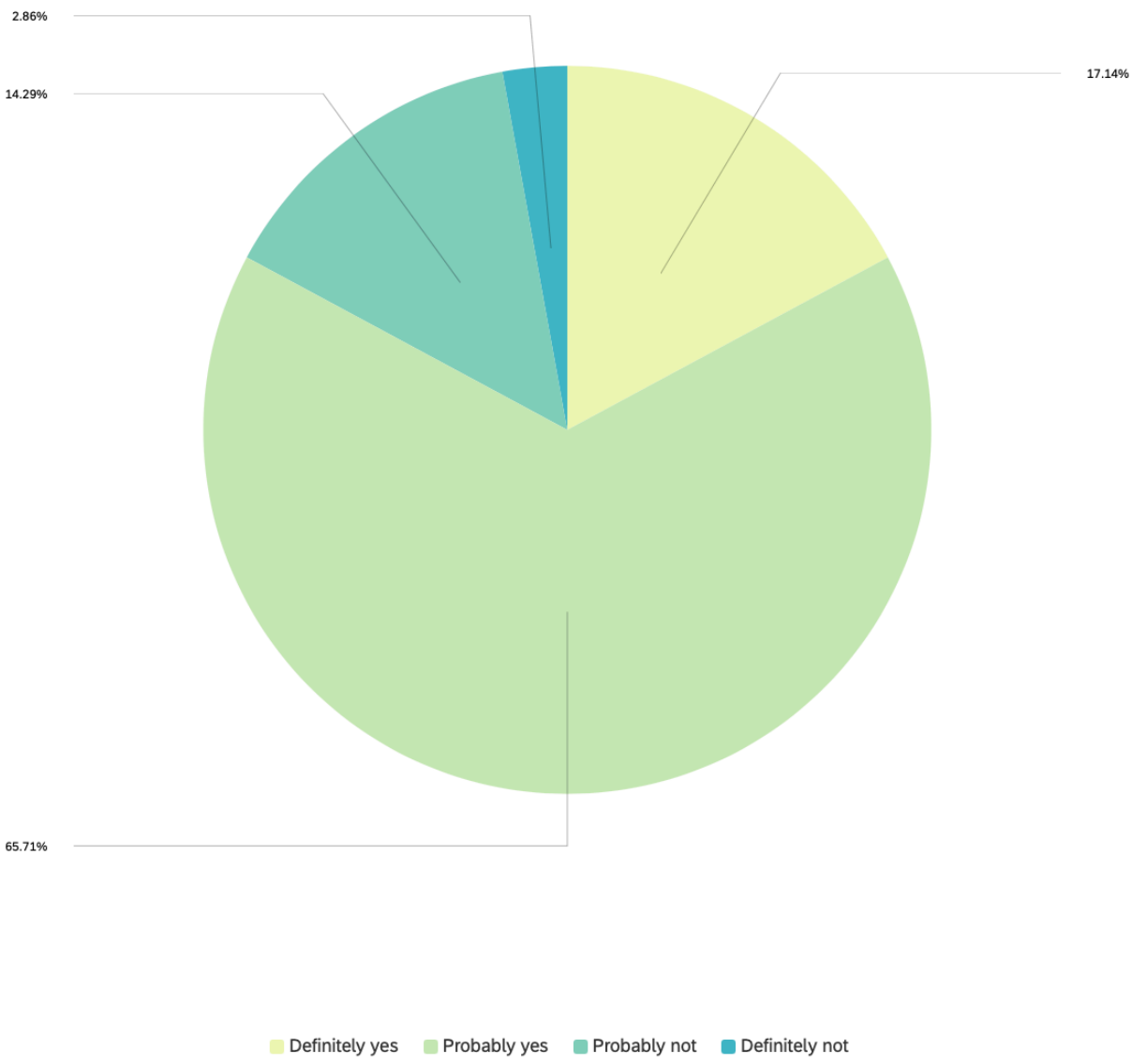
#	Field		Choice Count
1	Definitely yes	27.78%	10
2	Probably yes	47.22%	17
3	Probably not	22.22%	8
4	Definitely not	2.78%	1
			36



3) Will regulations strengthen IoT security?



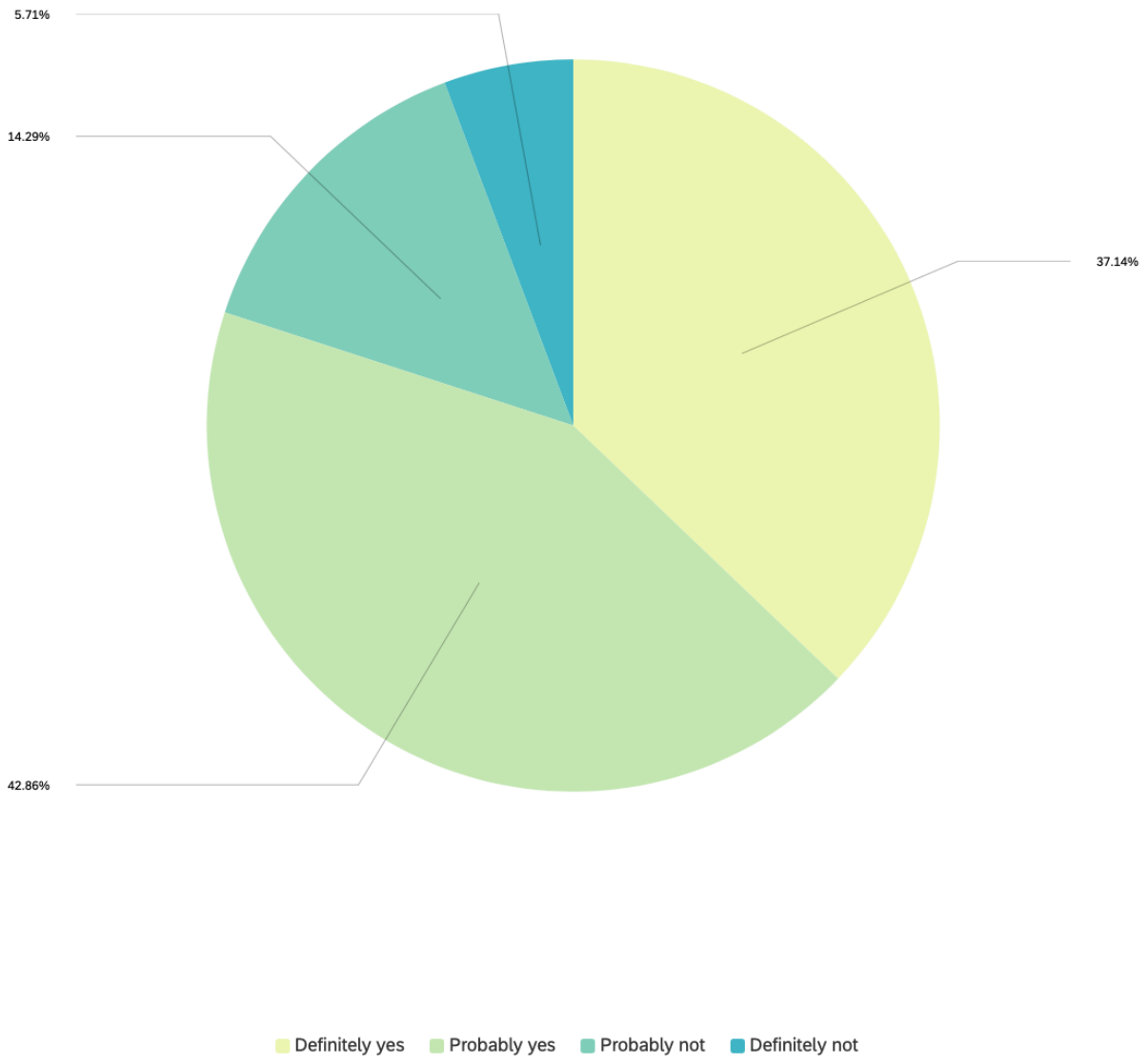
#	Field	Choice Count
1	Definitely yes	17.14% 6
2	Probably yes	65.71% 23
3	Probably not	14.29% 5
4	Definitely not	2.86% 1
		35



4) Will a common IoT security reference architecture strengthen IoT security?

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Will a common IoT security reference architecture strengthen IoT security? Select one.	1.00	4.00	1.89	0.85	0.73	35

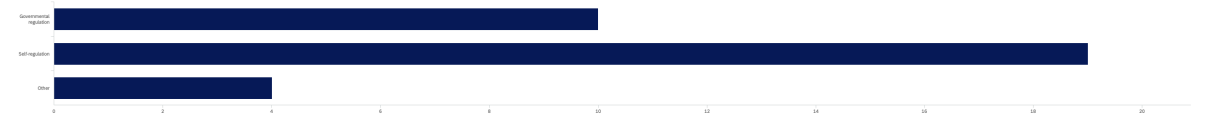
#	Field		Choice Count
1	Definitely yes	37.14%	13
2	Probably yes	42.86%	15
3	Probably not	14.29%	5
4	Definitely not	5.71%	2
			35



5) Which regulatory approach is suitable for IoT security?

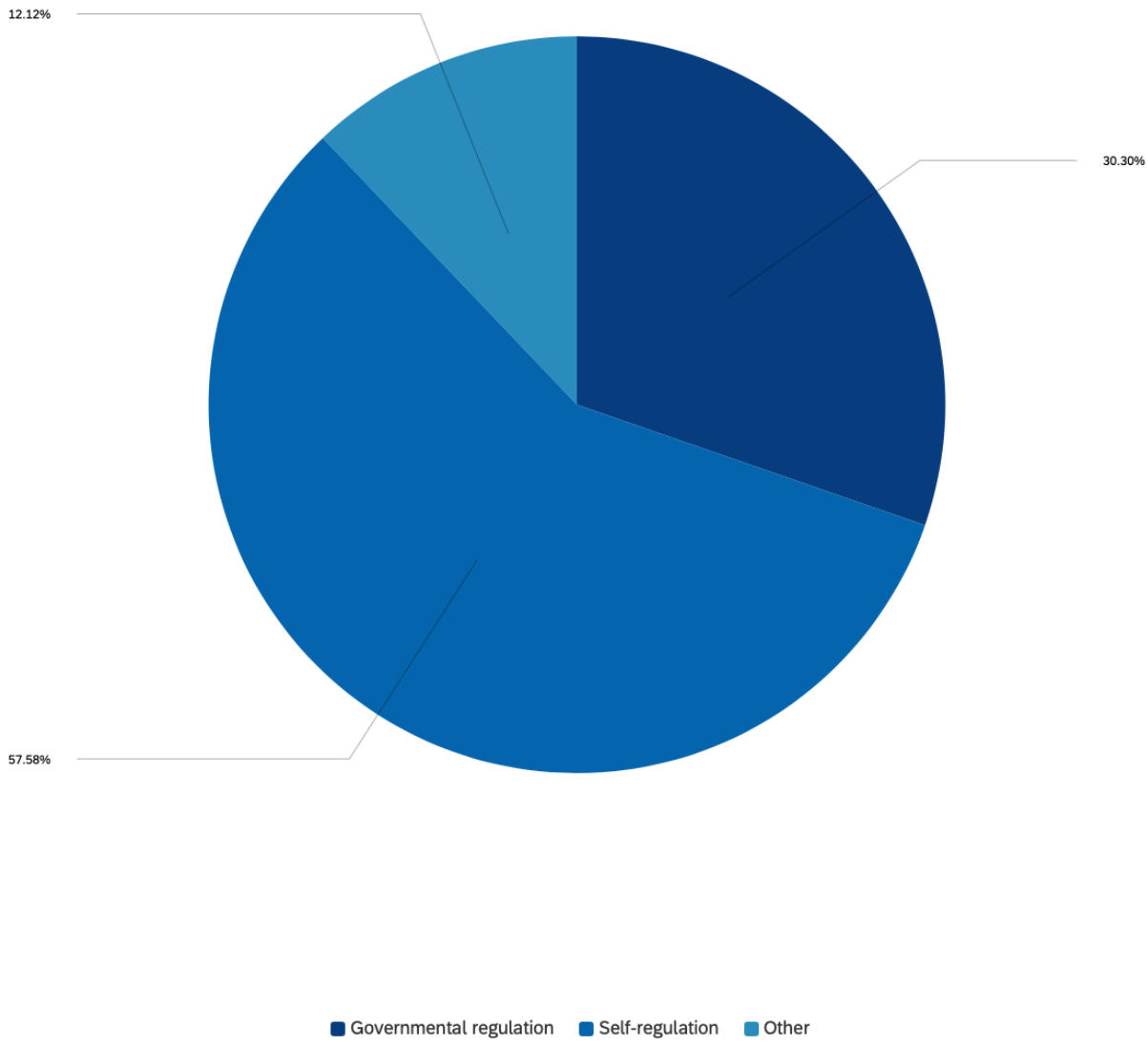
Q5 - Which regulatory approach is suitable for IoT security? Select one.

Page Options

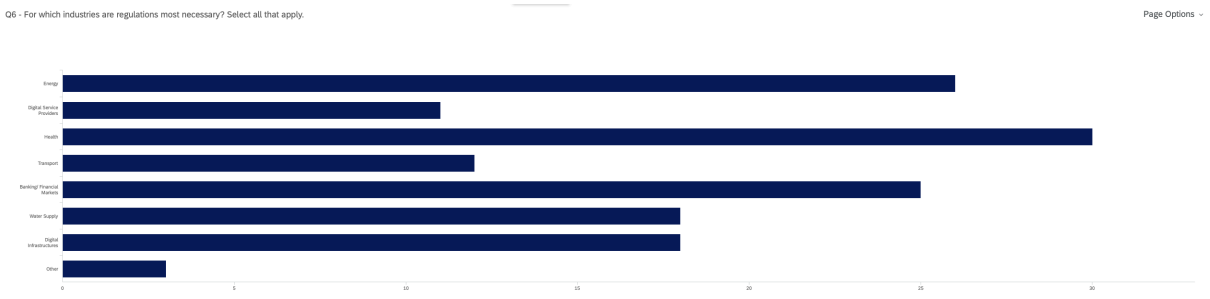


#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Which regulatory approach is suitable for IoT security? Select one. - Selected Choice	1.00	3.00	1.82	0.63	0.39	33

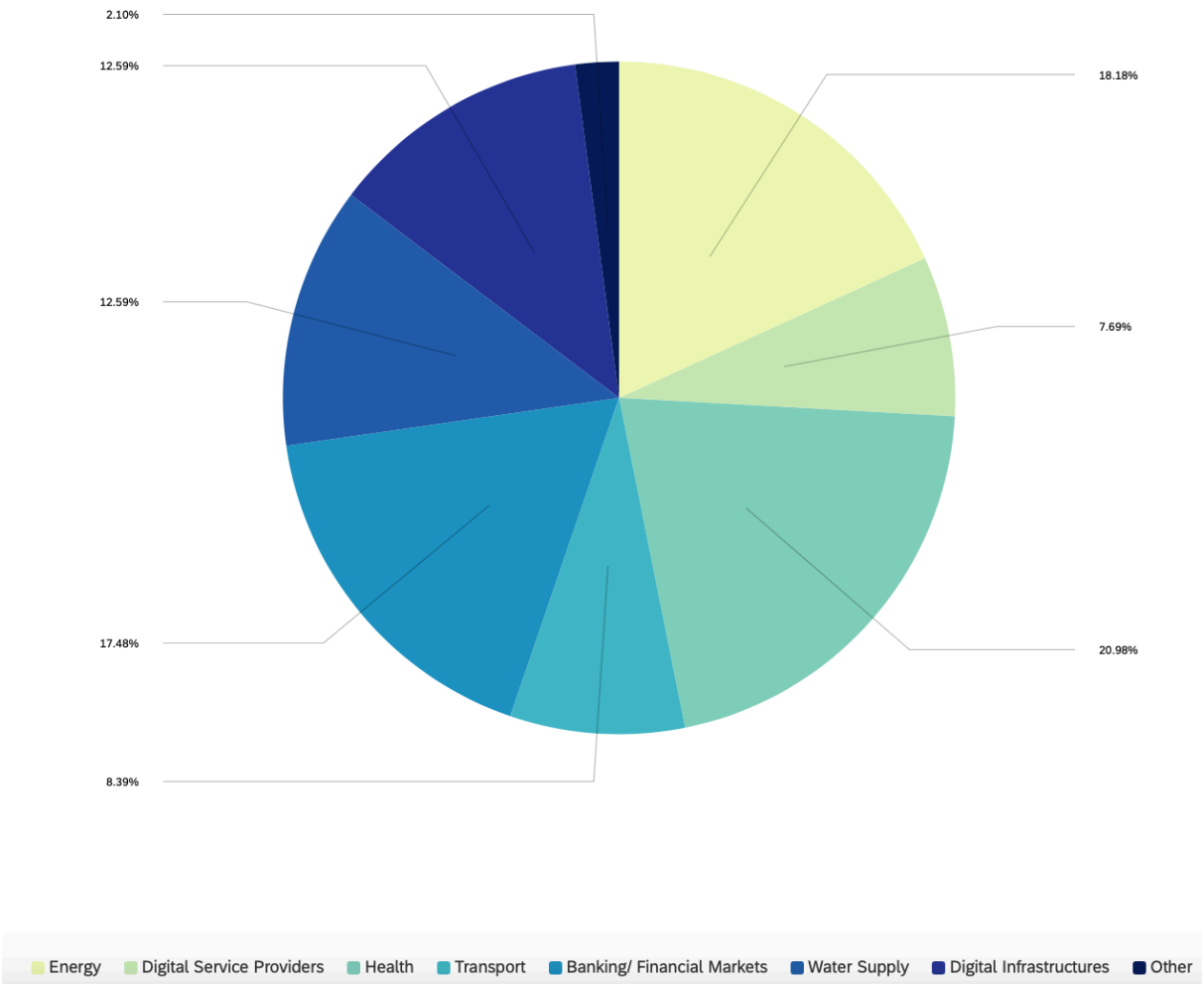
#	Field		Choice Count
1	Governmental regulation	30.30%	10
2	Self-regulation	57.58%	19
3	Other	12.12%	4
			33



6) For which industries are regulations most necessary?



#	Field	Choice Count	
1	Energy	18.18%	26
2	Digital Service Providers	7.69%	11
3	Health	20.98%	30
4	Transport	8.39%	12
5	Banking/ Financial Markets	17.48%	25
6	Water Supply	12.59%	18
7	Digital Infrastructures	12.59%	18
8	Other	2.10%	3
			143

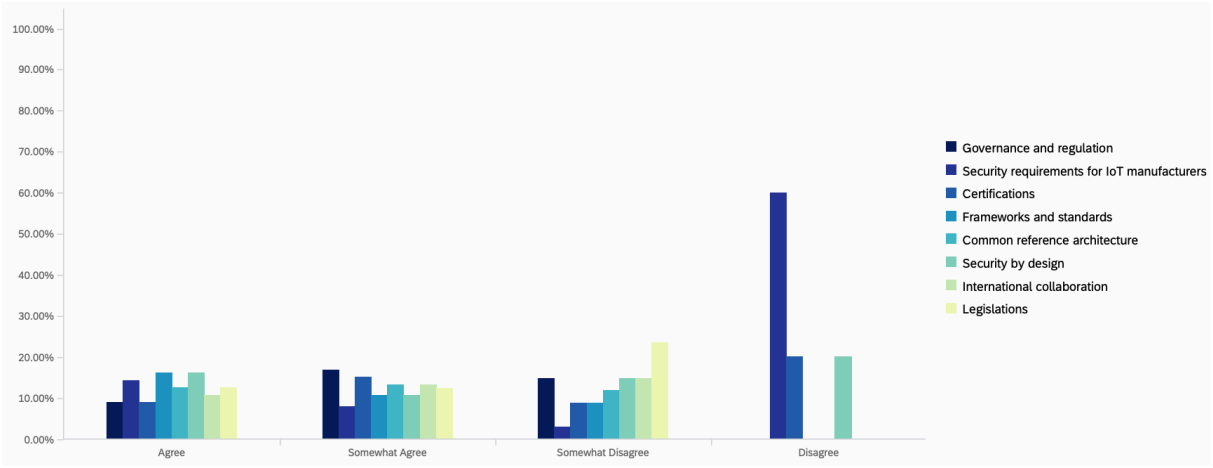


7) What measures can foster IoT security? Please rank each.

Q7 - What measures can foster IoT security? Please rank each.

Page Options

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Governance and regulation	1.00	3.00	2.00	0.59	0.34	29
2	Security requirements for IoT manufacturers	1.00	4.00	1.95	1.00	1.00	21
3	Certifications	1.00	4.00	2.00	0.68	0.46	26
4	Frameworks and standards	1.00	3.00	1.75	0.66	0.44	24
5	Common reference architecture	1.00	3.00	1.88	0.64	0.41	26
6	Security by design	1.00	4.00	1.93	0.81	0.66	27
7	International collaboration	1.00	3.00	1.96	0.65	0.42	26
8	Legislations	1.00	3.00	2.03	0.72	0.52	29

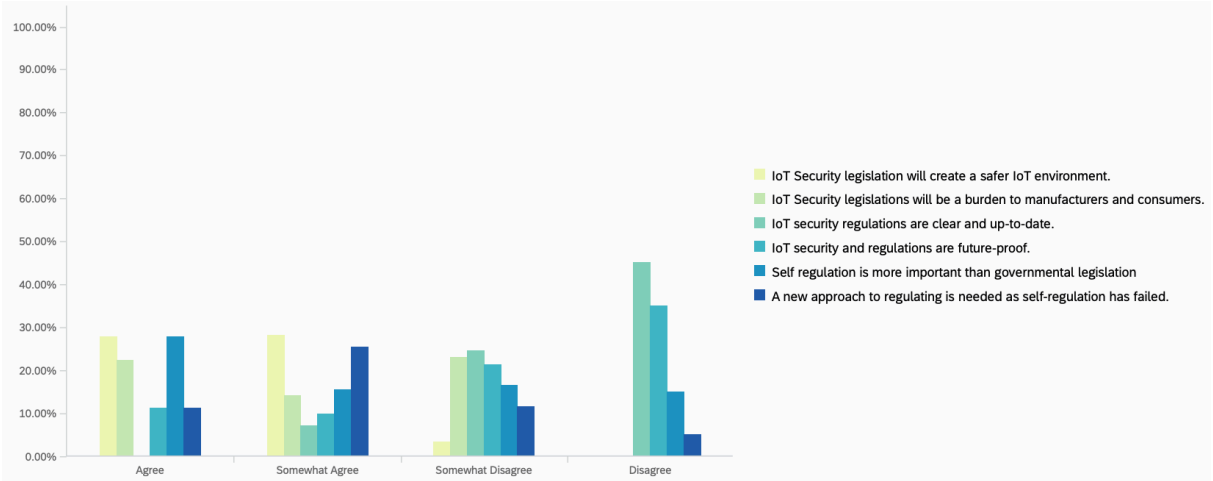


8) Please state your degree of approval. Please rank each.

Q8 - Please state your degree of approval. Please rank each.

Page Options

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	IoT Security legislation will create a safer IoT environment.	1.00	3.00	1.89	0.50	0.25	27
2	IoT Security legislations will be a burden to manufacturers and consumers.	1.00	3.00	2.36	0.72	0.52	28
3	IoT security regulations are clear and up-to-date.	2.00	4.00	3.14	0.68	0.46	29
4	IoT security and regulations are future-proof.	1.00	4.00	2.86	0.86	0.74	29
5	Self regulation is more important than governmental legislation	1.00	4.00	2.38	0.89	0.79	29
6	A new approach to regulating IoT Security is needed as self-regulation has failed.	1.00	4.00	2.25	0.63	0.40	28



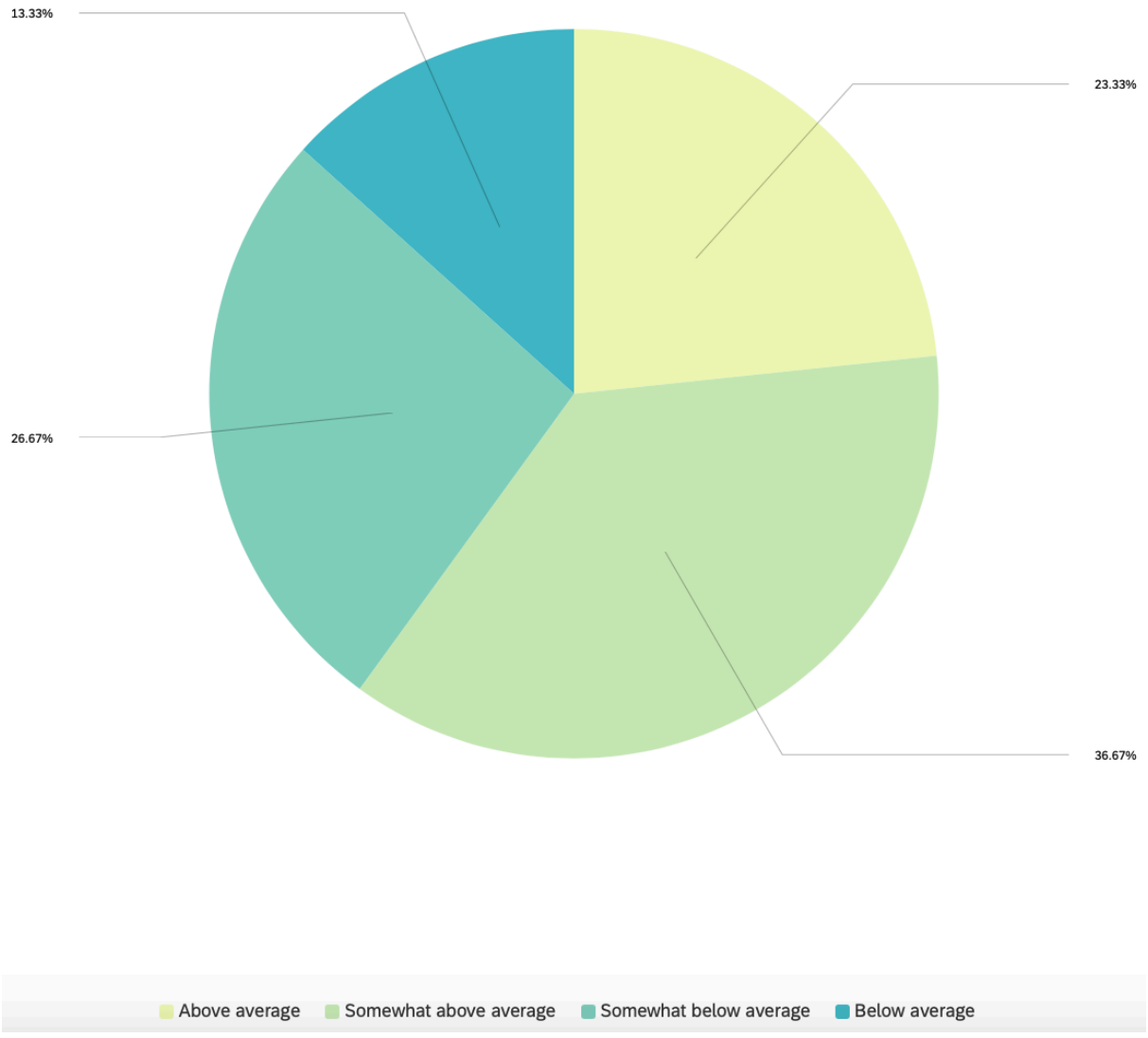
9) How would you rate your company's current maturity level regarding IoT Security?

Q9 - How would you rate your company's current maturity level regarding IoT Security? Select one.

Page Options

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	How would you rate your company's current maturity level regarding IoT Security? Select one.	1.00	4.00	2.30	0.97	0.94	30

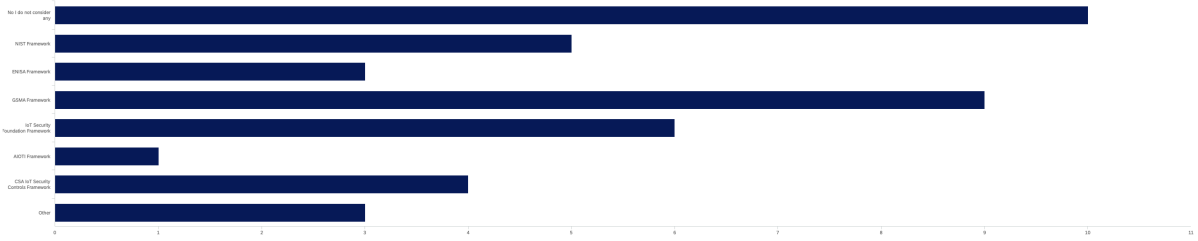
#	Field		Choice Count
1	Above average	23.33%	7
2	Somewhat above average	36.67%	11
3	Somewhat below average	26.67%	8
4	Below average	13.33%	4
			30



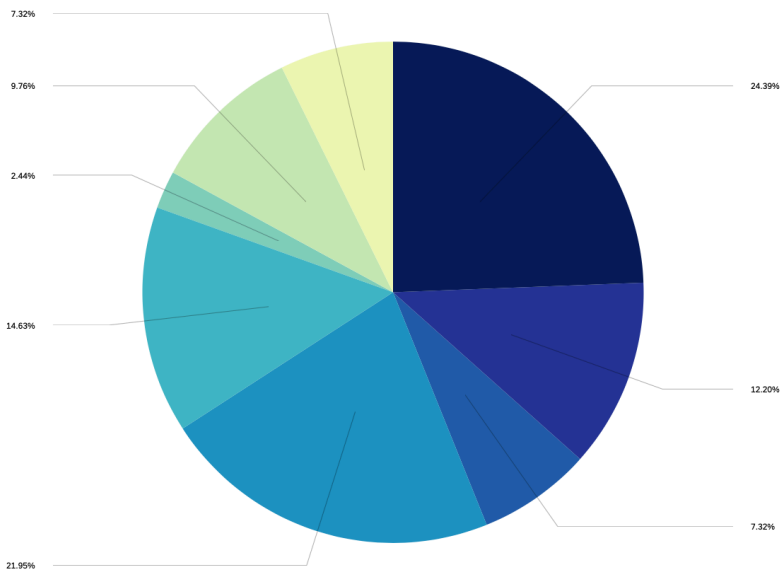
10) Do you currently consider any IoT security frameworks?

Q10 - Do you currently consider any IoT security frameworks? If yes, which ones? Select all that apply.

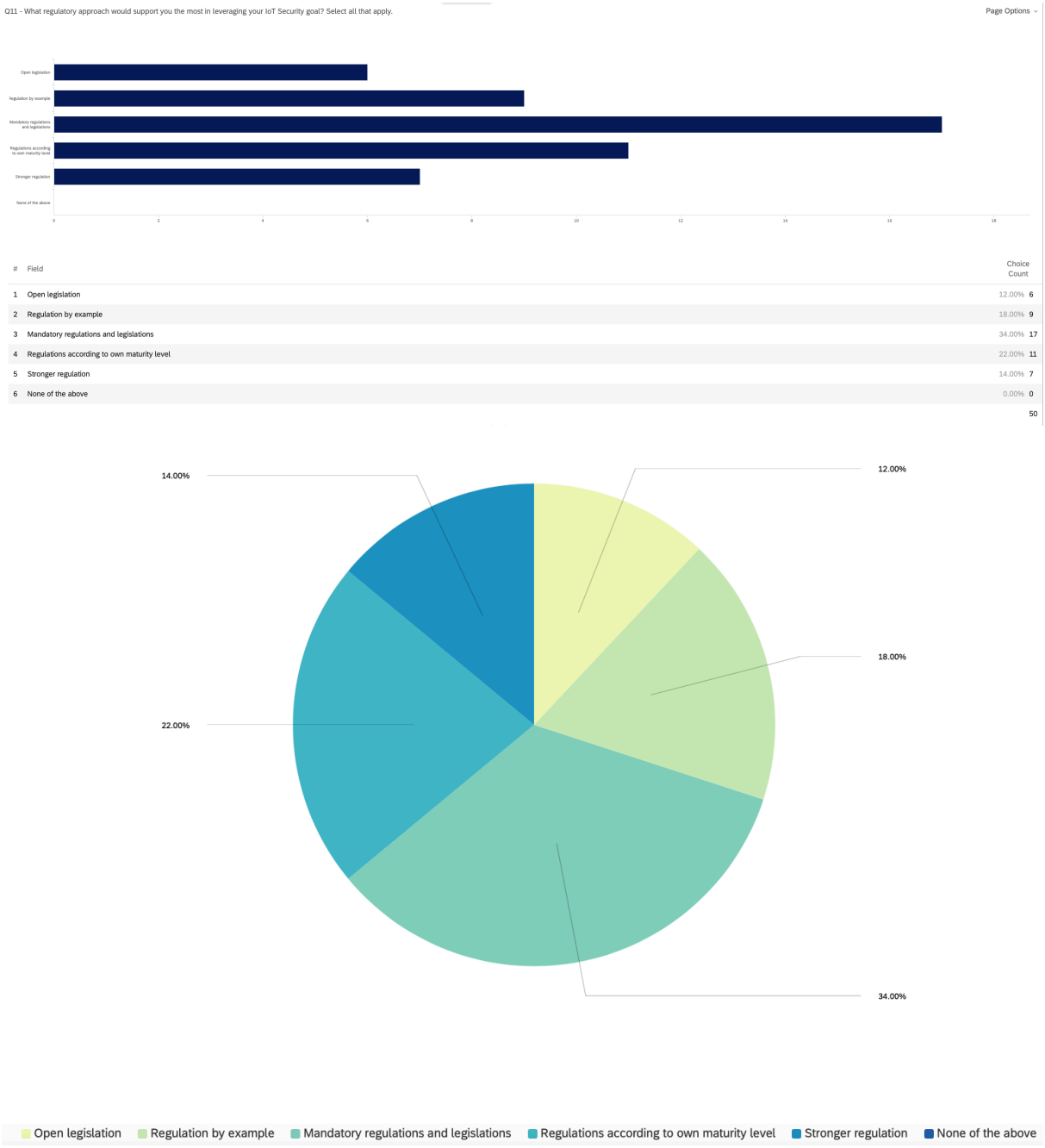
Page Options



#	Field		Choice Count
1	No I do not consider any	24.39%	10
2	NIST Framework	12.20%	5
3	ENISA Framework	7.32%	3
4	GSMA Framework	21.95%	9
5	IoT Security Foundation Framework	14.63%	6
6	AIOTI Framework	2.44%	1
7	CSA IoT Security Controls Framework	9.76%	4
8	Other	7.32%	3
			41



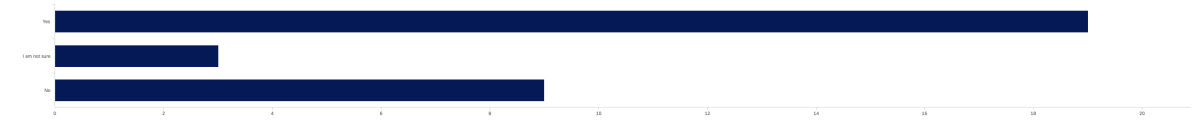
11) What regulatory approach would support you the most in leveraging your IoT Security goal?



12) Have you experienced a cyber security attack in your professional environment?

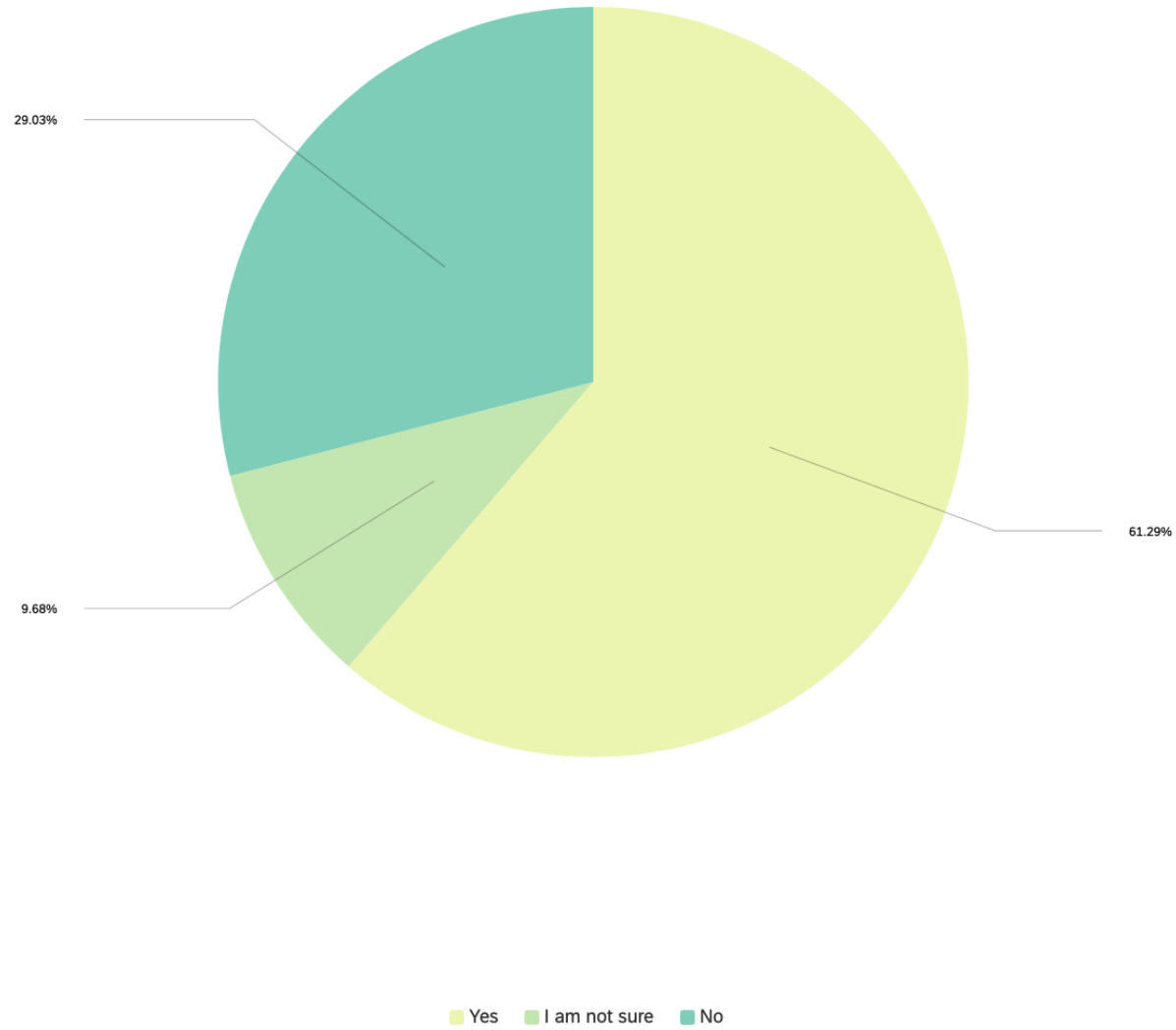
Q12 - Have you experienced a cyber security attack in your professional environment? Select one.

Page Options

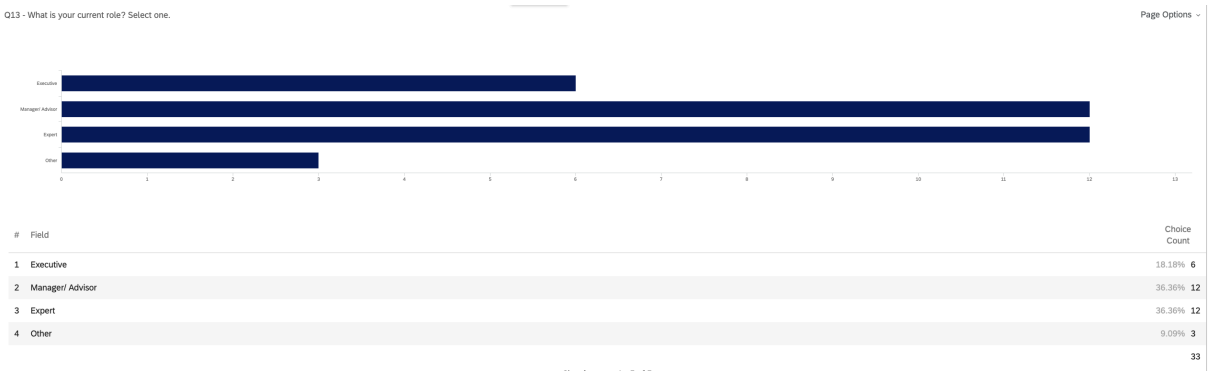


#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Have you experienced a cyber security attack in your professional environment? Select one.	1.00	3.00	1.68	0.89	0.80	31

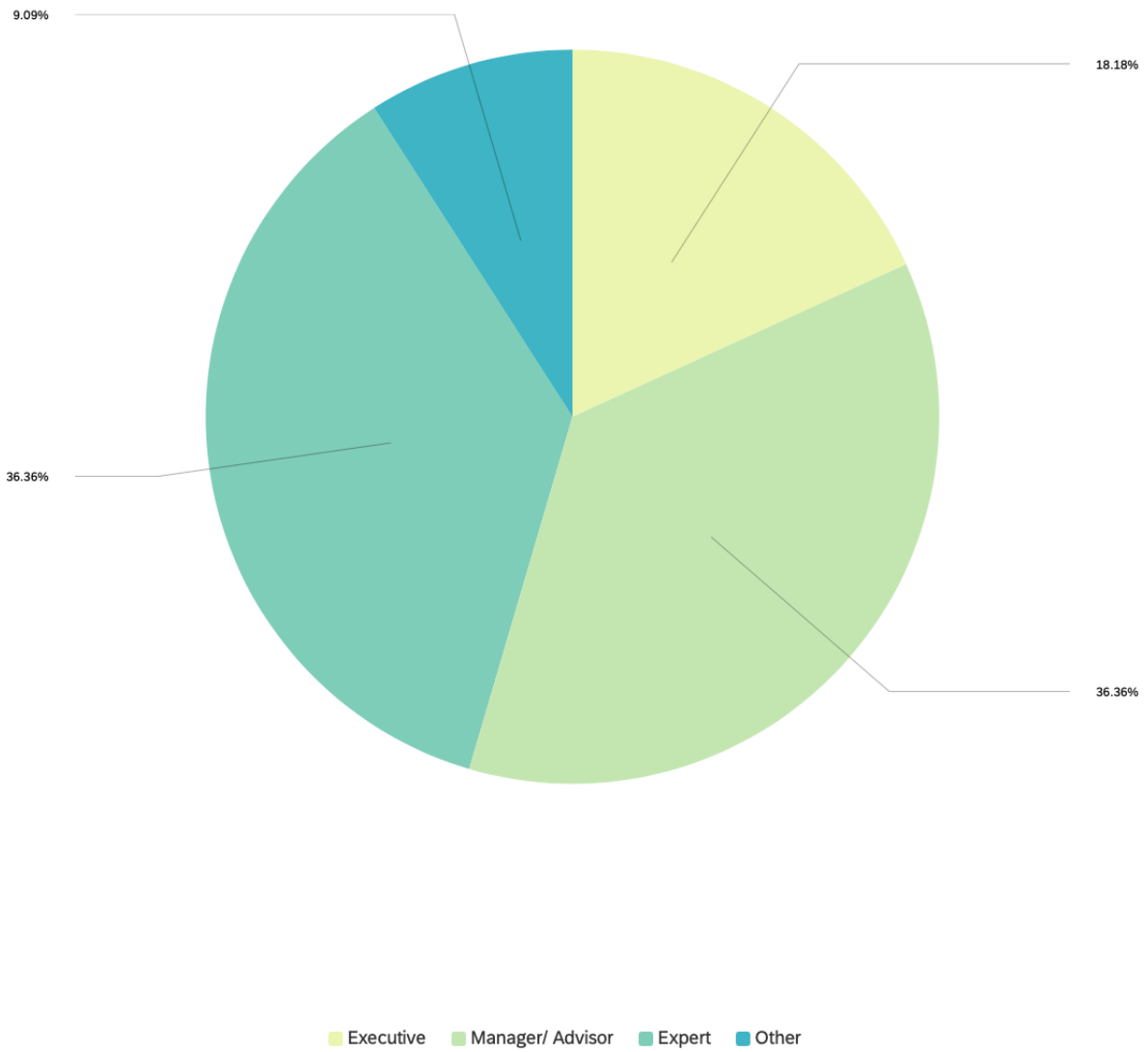
#	Field		Choice Count
1	Yes	61.29%	19
2	I am not sure	9.68%	3
3	No	29.03%	9
			31



13) What is your current role?



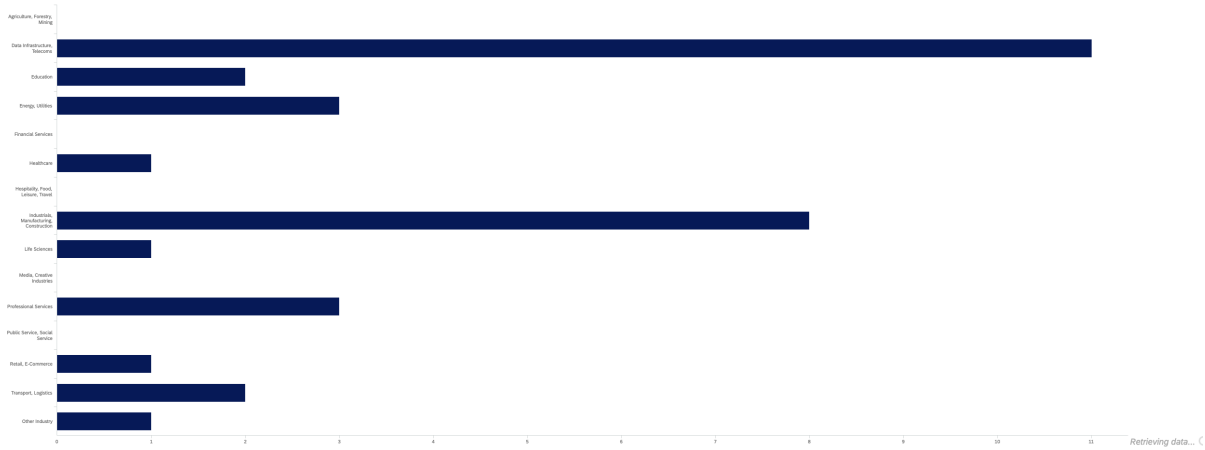
#	Field	Choice Count
1	Executive	18.18% 6
2	Manager/ Advisor	36.36% 12
3	Expert	36.36% 12
4	Other	9.09% 3
		33



14) In what sector are you currently working?

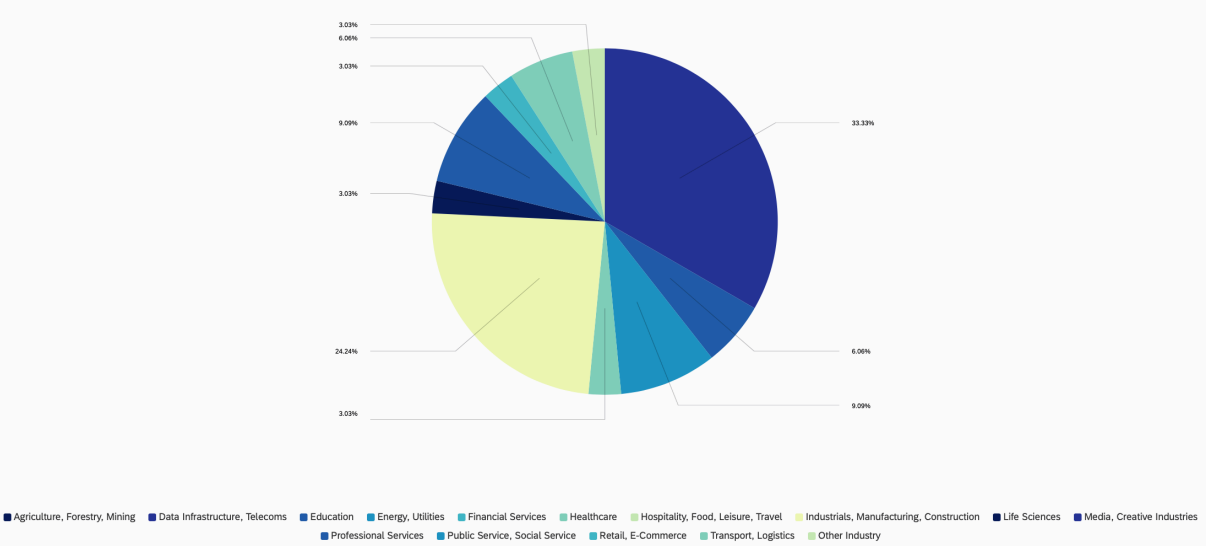
Q14 - In what sector are you currently working? Please select one.

Page Options



#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	In what sector are you currently working? Please select one.	2.00	15.00	6.30	4.18	17.48	33

#	Field	Choice Count	
1	Agriculture, Forestry, Mining	0.00%	0
2	Data Infrastructure, Telecoms	33.33%	11
3	Education	6.06%	2
4	Energy, Utilities	9.09%	3
5	Financial Services	0.00%	0
6	Healthcare	3.03%	1
7	Hospitality, Food, Leisure, Travel	0.00%	0
8	Industrials, Manufacturing, Construction	24.24%	8
9	Life Sciences	3.03%	1
10	Media, Creative Industries	0.00%	0
11	Professional Services	9.09%	3
12	Public Service, Social Service	0.00%	0
13	Retail, E-Commerce	3.03%	1
14	Transport, Logistics	6.06%	2
15	Other Industry	3.03%	1
			33



G. ArchiMate Models

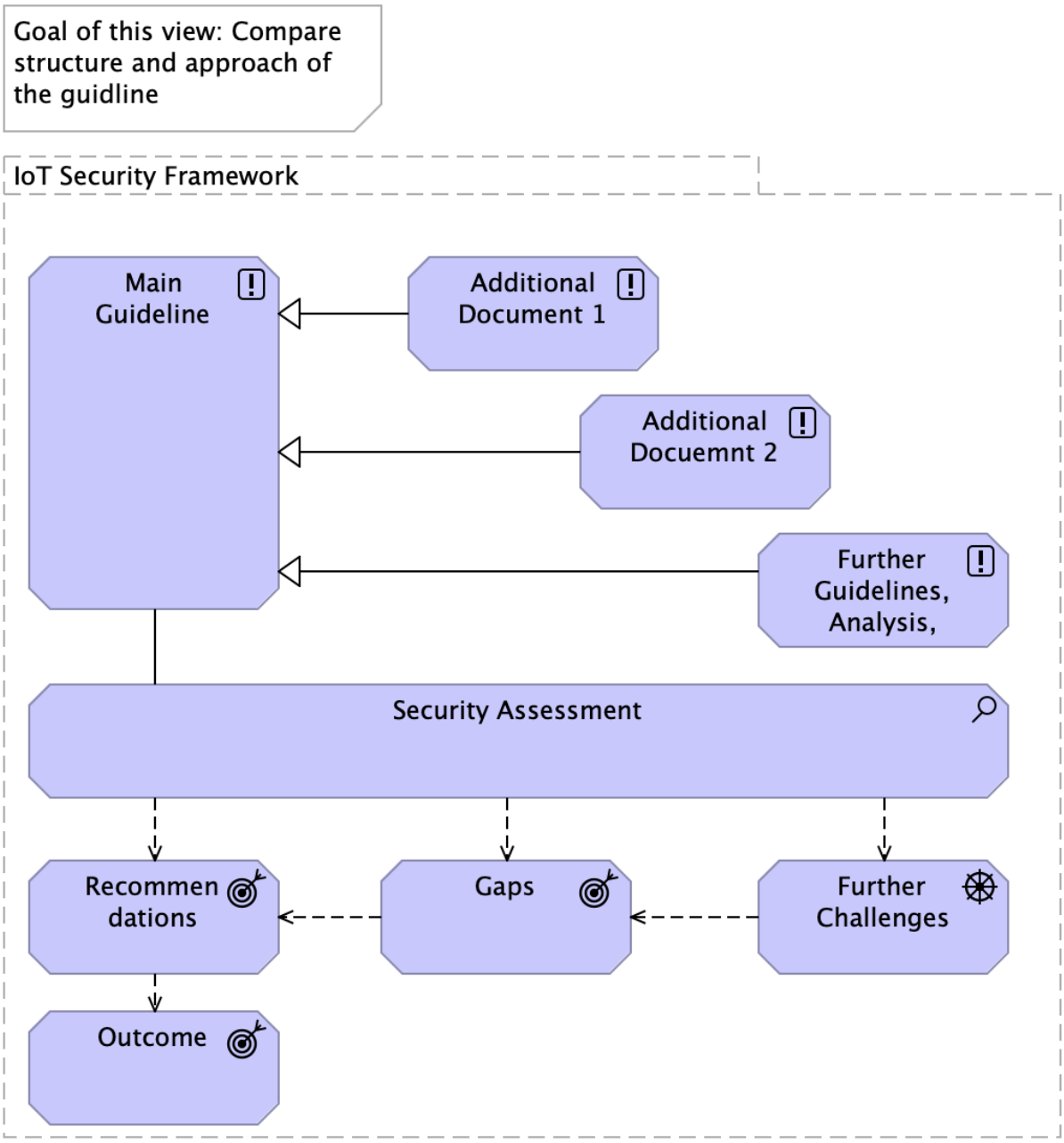


Figure 12: Viewpoint Metamodel Guideline Structure

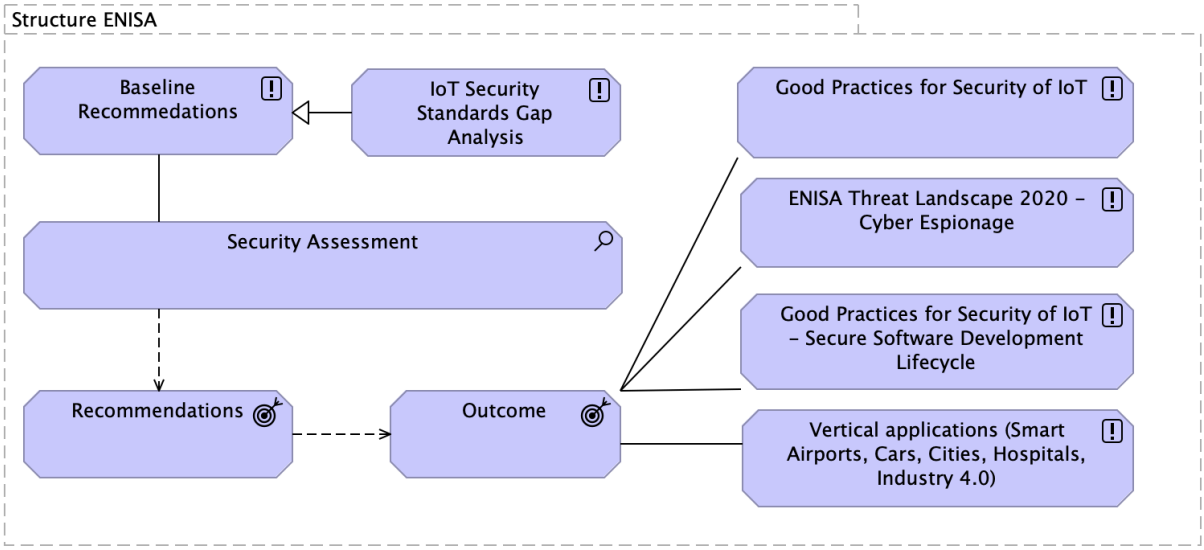


Figure 13:Viewpoint Guideline Structure ENISA

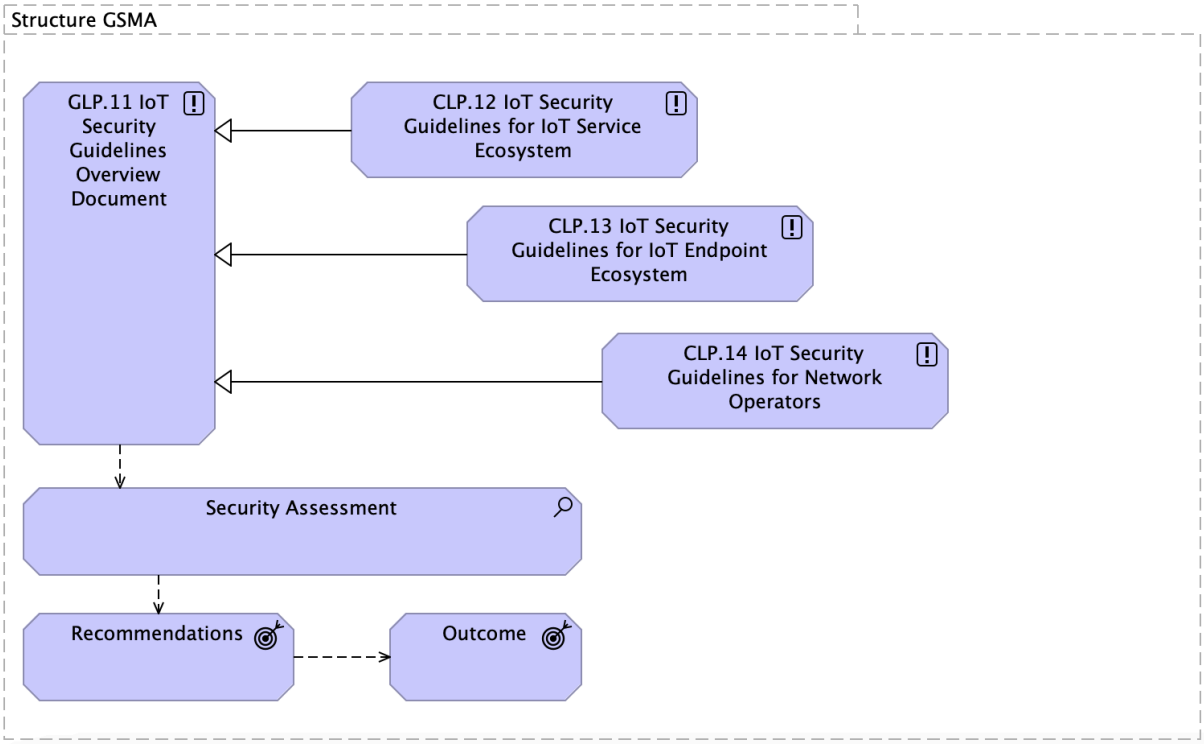


Figure 14: Viewpoint Guideline Structure GSMA

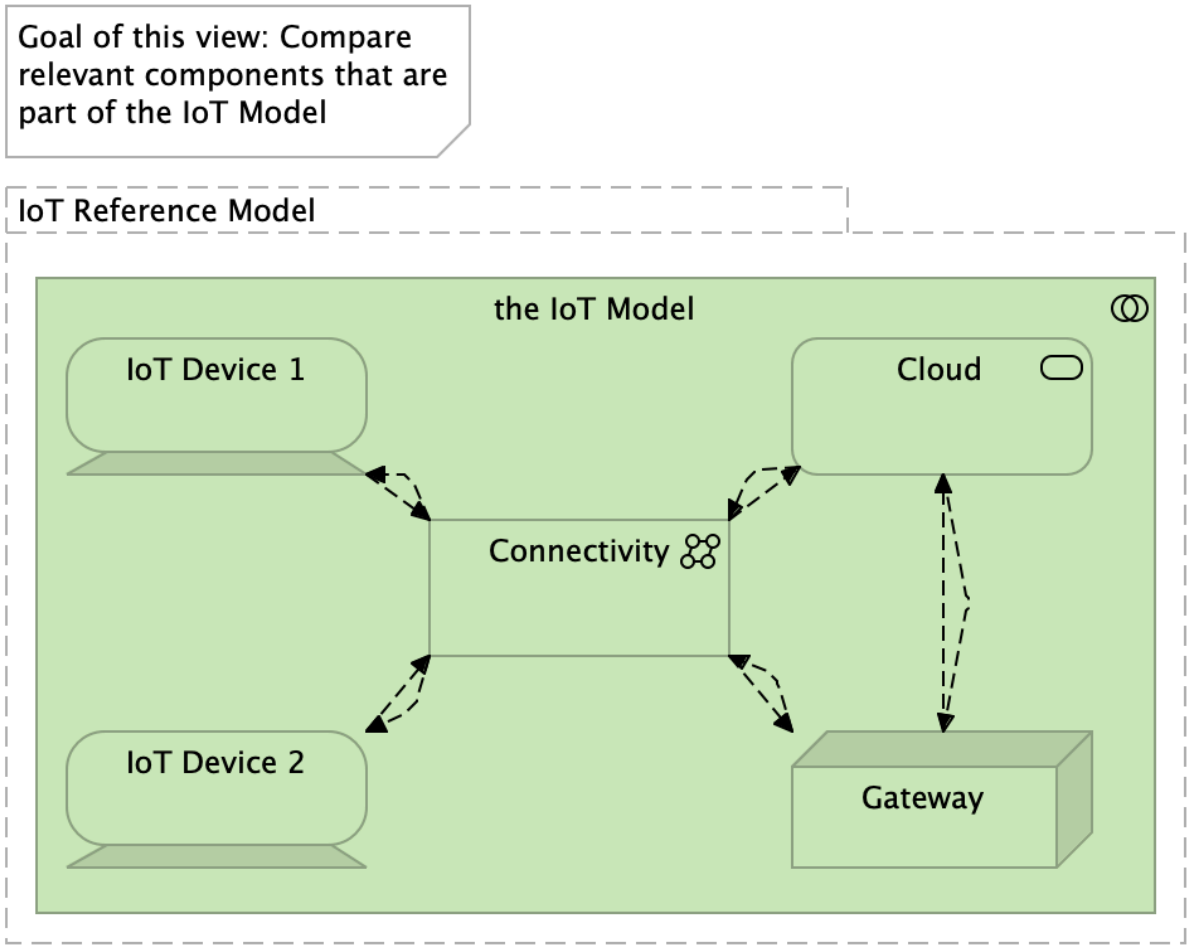


Figure 15: Viewpoint Metamodel IoT Model

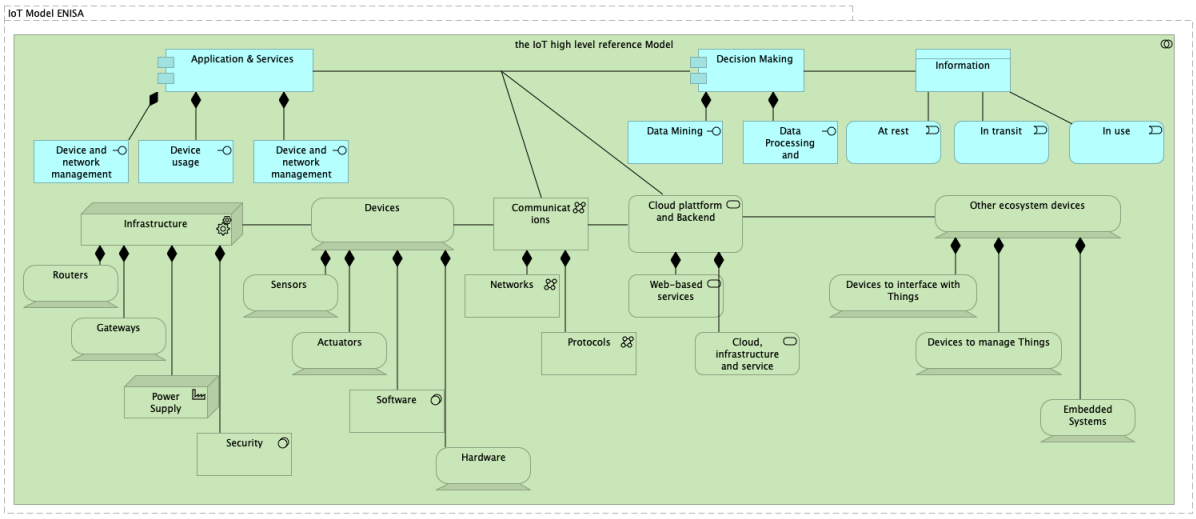


Figure 16:Viewpoint IoT Model ENISA

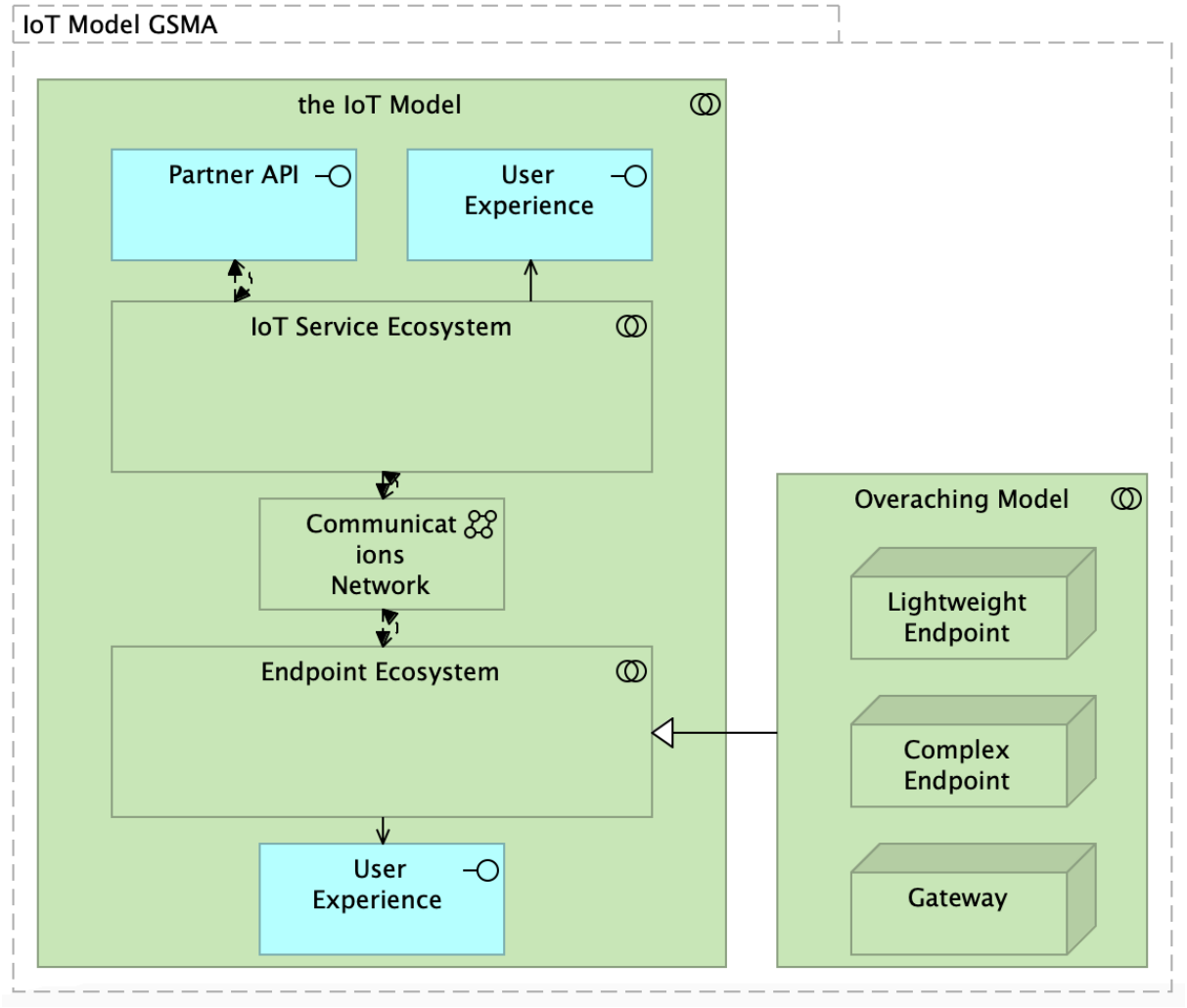


Figure 17: Viewpoint IoT Model GSMA

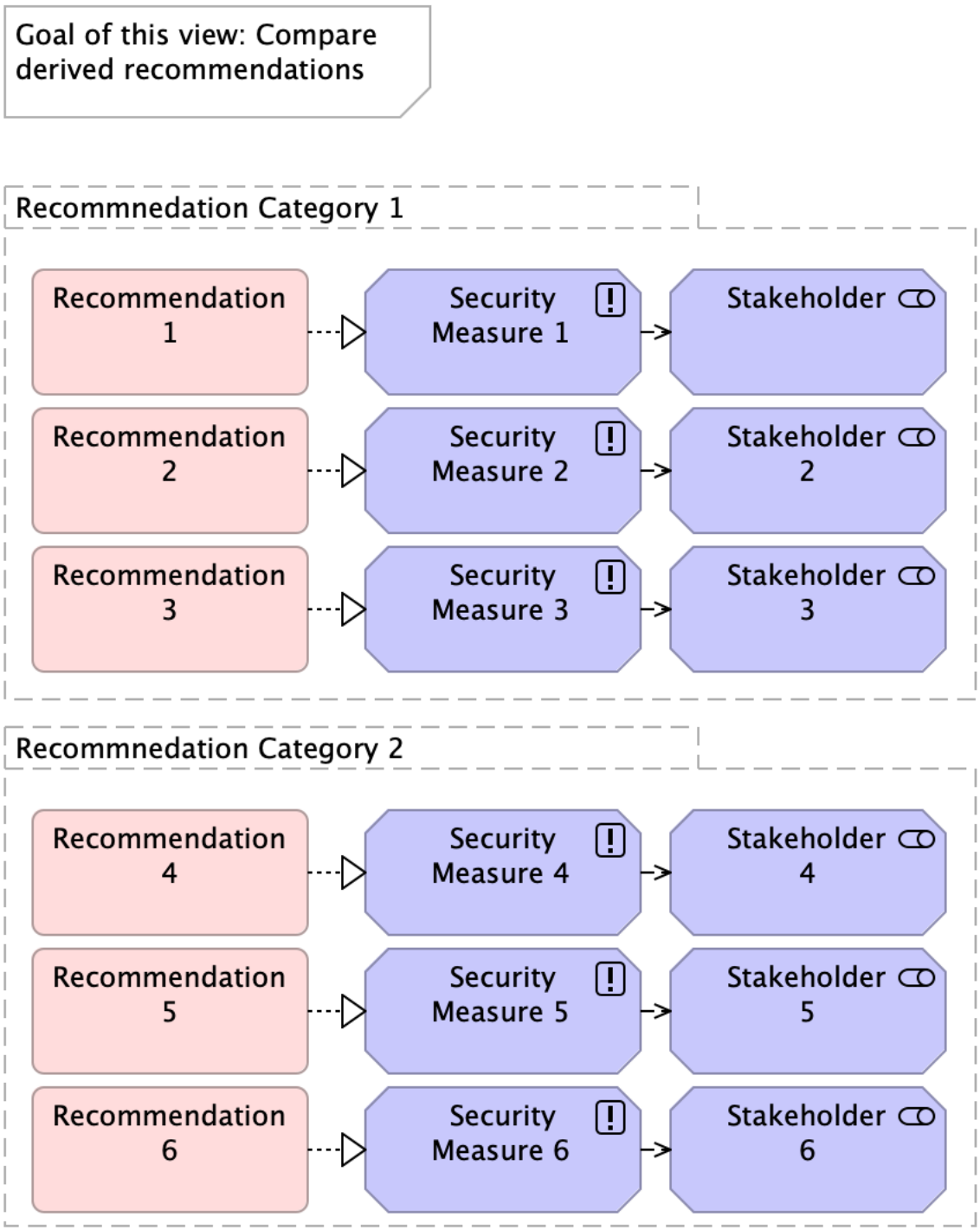


Figure 18: Viewpoint Metamodel Recommendations

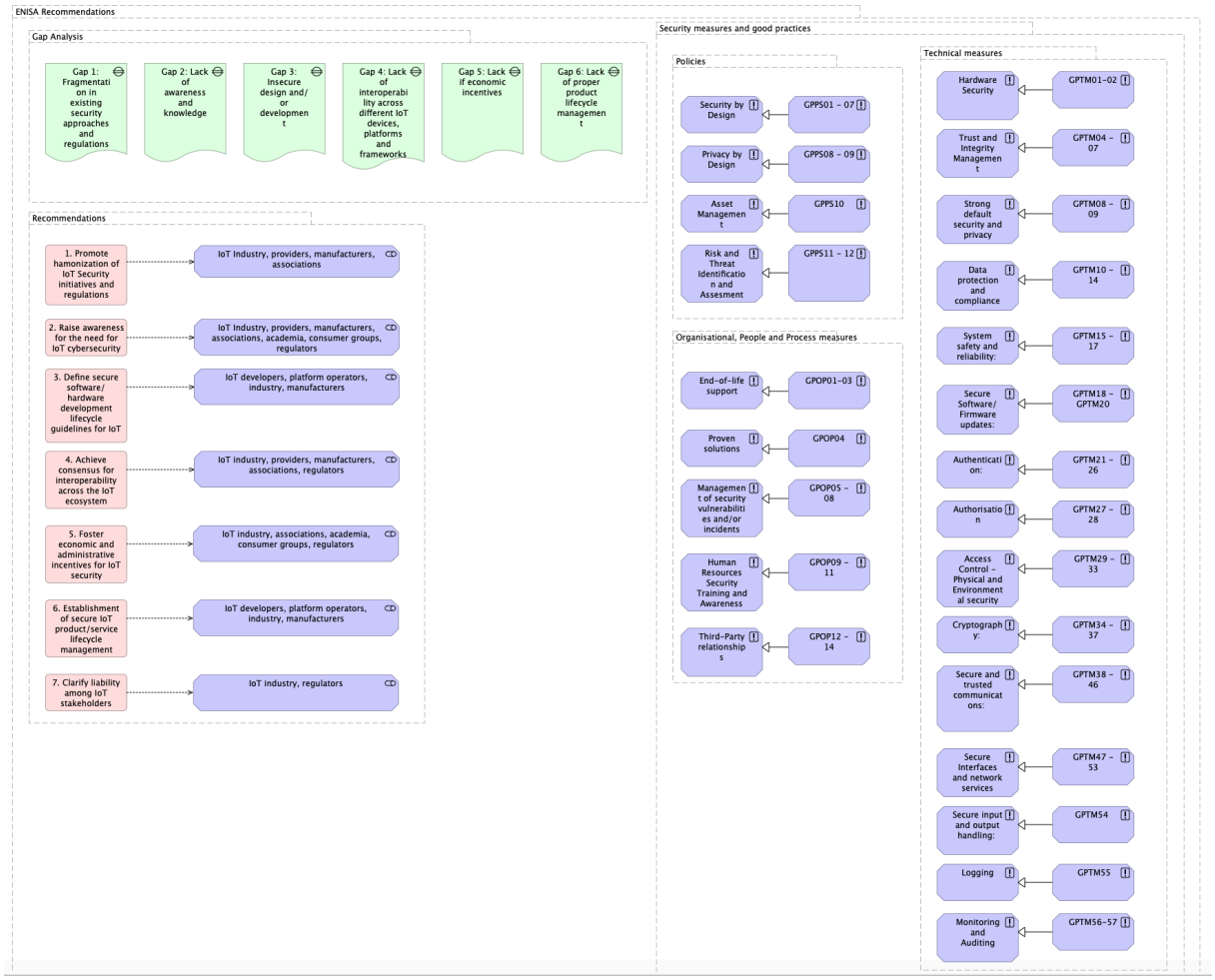


Figure 19: Viewpoint Recommendations ENISA

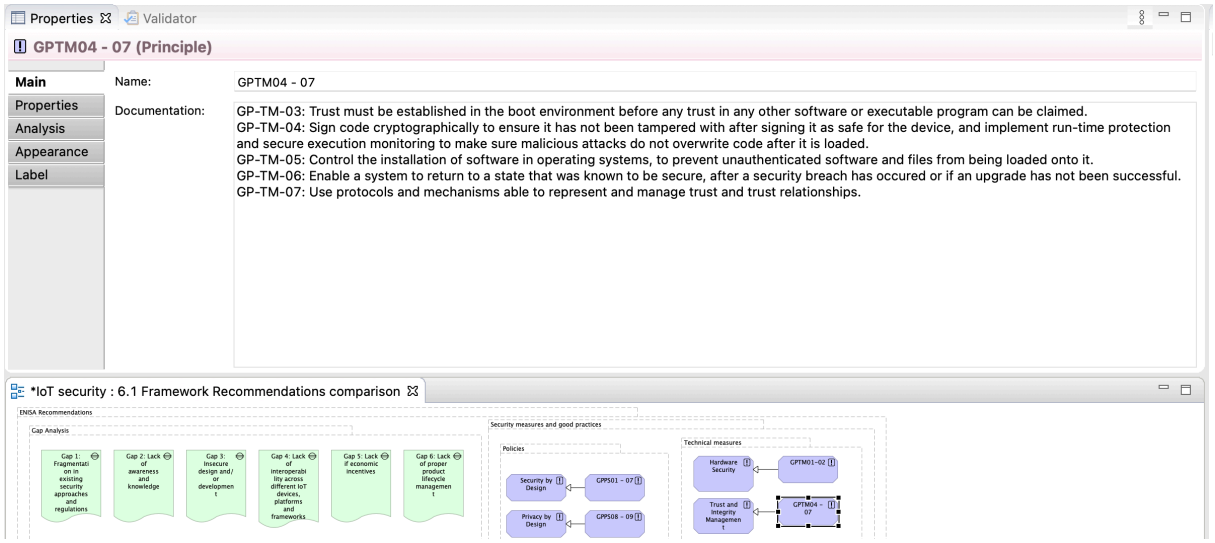


Figure 20: Example of detailed Recommendations in Documentation

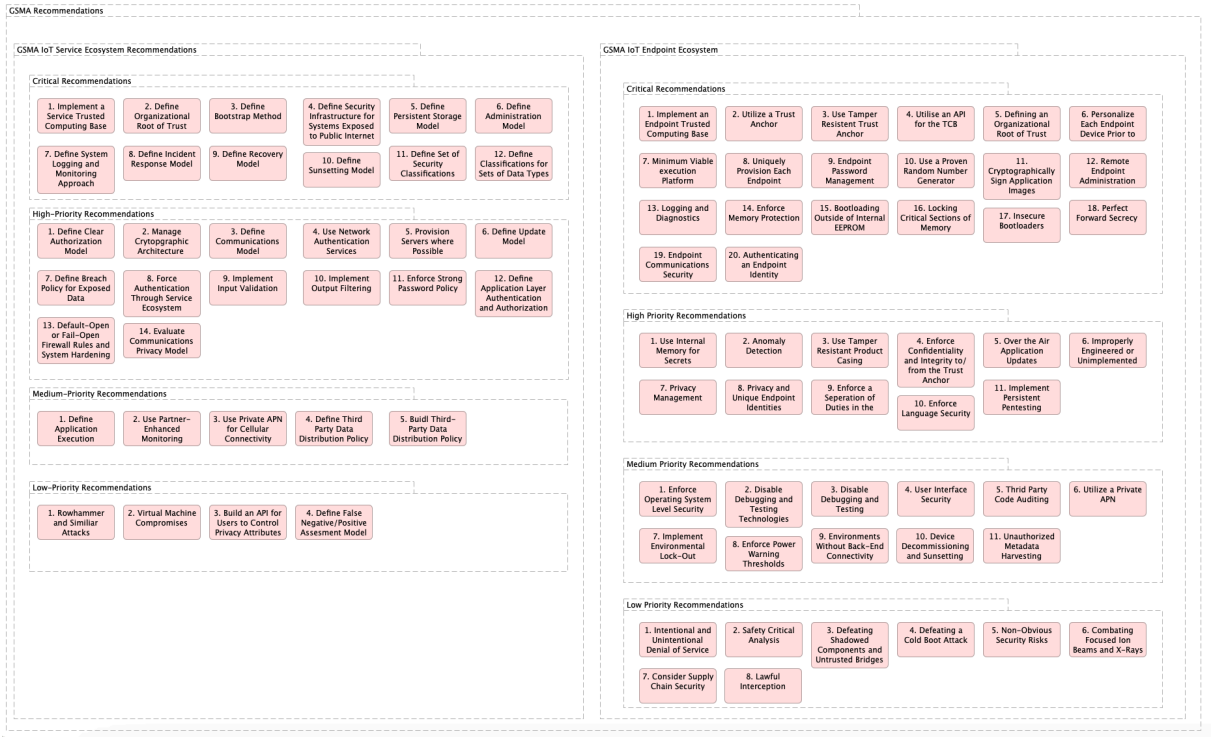


Figure 21: Viewpoint Recommendations GSMA

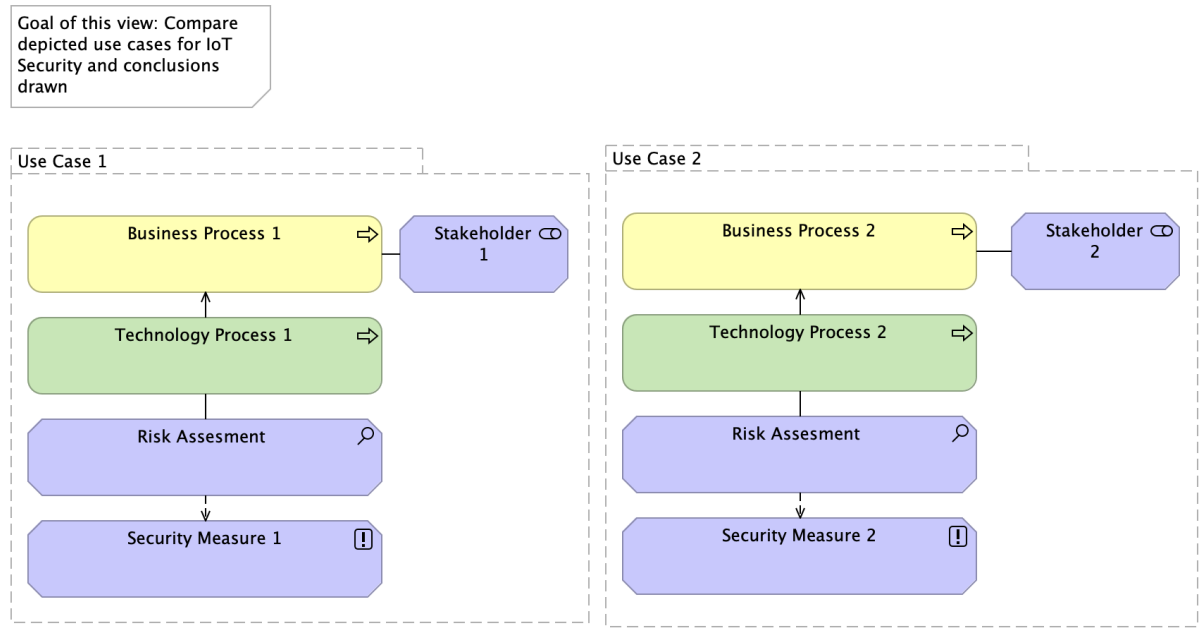


Figure 22: Viewpoint Metamodel Use Case

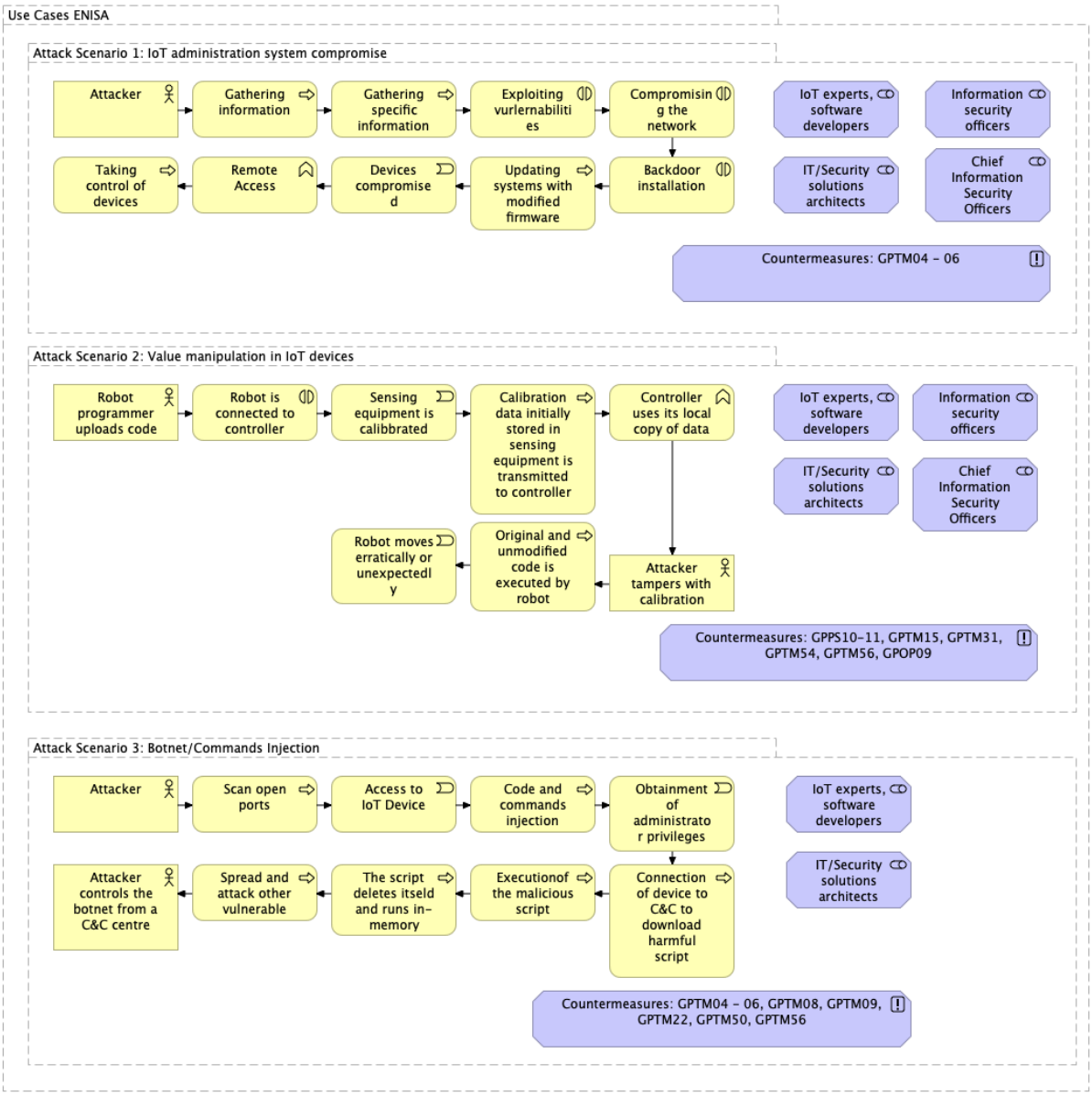


Figure 23: Viewpoint Use Case ENISA

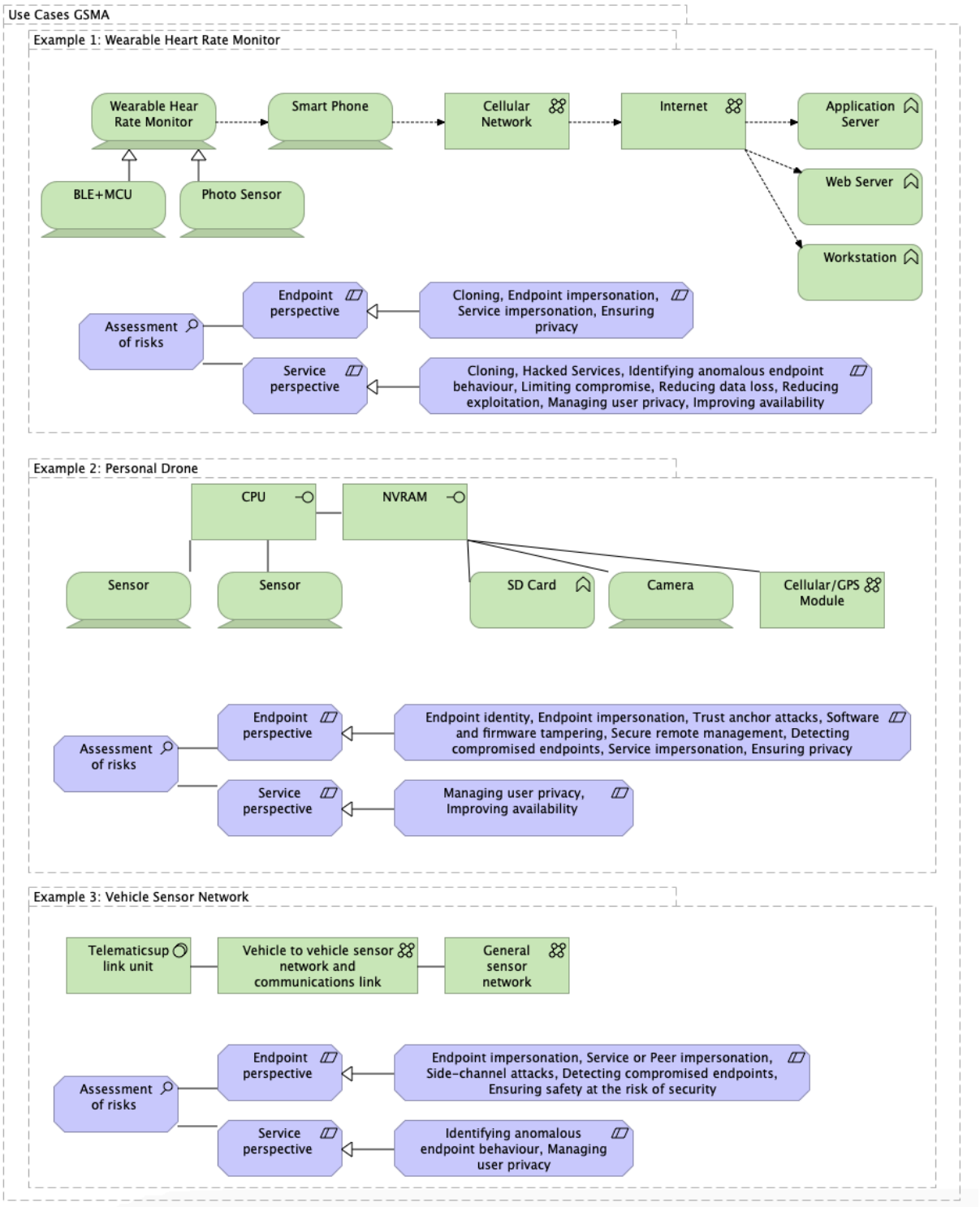


Figure 24: Viewpoint Use Case GSMA