Towards a cybersecurity assessment framework for IoT-based environments

THESIS CONCEPT VERSION 1.2

submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE
in
ICT IN BUSINESS

Author :	Luit Verschuur
Student ID :	1811053
Supervisor :	Prof. Dr. S. Pickl
2^{nd} corrector :	Prof. Dr. N. Mentens

Leiden, The Netherlands, May 20, 2022

Acknowledgments

This thesis was written under the supervision of Prof. Dr. Stefan Pickl, who I would like to thank for his intensive support throughout the project and the clear guidance he provided. Besides, I would like to thank Suzie Bernards. She has been the supervisor of my thesis internship at PwC NL and she helped me throughout the project with everything I needed from the company. Within the company, I was able to get in contact with a lot of interesting experts on IoT and cybersecurity. I want to thank them for the time and effort they have invested in my project. Last, I want to thank my dad for thinking along with me and going through my thesis to get everything on paper in the right way.

Towards a cybersecurity assessment framework for IoT-based environments

Luit Verschuur

Leiden Institute of Advanced Computer Science, Leiden University
Snellius Building, Niels Bohrweg 1, 2333 CA Leiden

May 20, 2022

Abstract

Today, our world is more connected than ever. One of the main drivers of this connection is the uprise of the Internet of Things (IoT). Associated with this rise, there are numerous challenges. One of the main challenges for IoT is to keep the environments that include IoT devices secure. IoT devices are different from traditional computer devices and therefore need special treatment and guidance to be kept secure. This research identifies the limitations of current assessment frameworks to cover IoT-specific challenges. It discusses the possible assessment methods to assess these challenges. In addition, the potential solutions to secure these environments are listed. Afterward, the processes and guidelines that can be implemented are identified. All to generalize these findings into an overall applicable cybersecurity assessment framework for IoT-based environments. Based on existing IoT frameworks, research, and interviews with experts this assessment framework is validated to guide IoT-based environments to improve their security.

Keywords: Internet of Things (IoT) · IoT-based environments · IoT specific challenges · security and protection · assessment methods · cybersecurity assessment framework

Contents

Special Terms

availability Ensuring timely and reliable access and guaranteeing the use of information [Hou11].

biometrics The use of unique personal characteristics, like fingerprints and face recognition, to authenticate the user.

blockchain A technique that uses a growing list of data structures, called blocks, that are connected and secured by cryptography [BFL20].

CFAM Cyber Forensic Assurance Model [Dar10].

chain of trust The chain in which every part plays its role to provide security. When every part does its job to secure it it will be secure. However when one part fails to do so the whole chain fails. Therefore, every part must trust the others to provide security..

CIA triad A benchmark for evaluating the effectiveness of information systems security, based on three primary objectives of any security program: Confidentiality, Integrity and Availability [Fen08].

CMM Capability Maturity Model [Pau+93].

confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [Hou11].

CPRA The California Privacy Rights Act.

cryptography The scientific study of techniques that secure digital information, transactions and distributed computations [KL20].

cybersecurity The practice of protecting critical systems and sensitive information from digital attacks [IBM22].

EAR Encryption At Rest.

ECC Elliptic Curve Cryptography, an approach to public-key cryptography.

EIT Encryption in Transit.

ENISA The European Union agency for cybersecurity.

ETSI European Telecommunications Standards Institutes.

GDPR The General Data Protection Regulation.

grounded theory The most accepted method used to process qualitative data.

groupthink The mode of thinking that people engage in when they are deeply involved in a cohesive in-group. This results in members that strive for unanimity and override their personal motivation [Jan08].

IDS Intrusion detection system.

integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity [Hou11].

intermediate labeling A method created to determine questions in interviews based on insights that are retrieved in previous interviews.

IoT Internet of Things, is a network that consists of physical objects that are connected with sensors, software, and other technologies. This connection of physical objects is realized over the internet and focuses mainly on exchanging data [Ora20].

IoT devices The union of IoT devices and operational technologies.

IoT-based environments The combination of all IoT devices, operational technologies and the IoT platform. These three components are part of the PwC IoT Cyber Security Triad and cover the whole set of connected devices in one environment [PwC22].

IoT-CIA The IoT-Cybersecurity Improvement Act.

IoTSF IoT Security Foundation.

ISO/IEC An international standard on how to manage information security. Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

lightweight encryption An encryption method that features a small footprint and/or low computational complexity [Tos17].

malicious actors Users who intentionally access a system with the intent to cause harm to the system or to use it in an unauthorized manner.

malware Short for malicious software that encompasses viruses, trojans, spyware and other intrusive code [VY06].

NIST National Institute of Standards and Technology of the United States.

non-repudiation Assurance that the sender of information is provided with proof of delivery [SHB06].

open coding A qualitative approach to code concepts discussed in the data.

OSI The Open Systems Interconnection model (OSI model), is the model that describes the standards for communication functions over a computer system.

Principle of Least Privilege A subject should be given only those privileges needed for it to complete its task. If a subject does not need an access right, the subject should not have that right. Further, the function of the subject (as opposed to its identity) should control the assignment of rights [VM01].

quantitative metrics The use of a certain formula to measure the relevant values.

research for design A research method that is based on the design of something.

security by design Focus on providing security, starting at the design of the IoT product.

steganography Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means ”covered writing” [JJ98].

TCP/IP TCP is a reliable transport protocol tuned to perform well in traditional networks made up of links with low bit-error rates [Bal+95].

tenet A principle or belief, especially one of the main principles of a religion or philosophy.

traditional computing devices A collective name for among other things computers, laptops and mobile phones. Indicating the former situation where only the most powerful computing devices had a link to the internet.

vendor A person or company offering something for sale, in IoT-based environments this is often the supplier of the IoT device.

Chapter 1

Introduction

In this chapter, a general introduction to this research project is given. This is done with the help of an outline of the following sections: research context, research objective, research relevance, research questions, research scope, and research structure.

1.1 Research context

Today, our world is more connected than ever. This connection is continuously spurred by technological advancements. One of the main advancements in recent years was the upcoming of the Internet of Things (IoT). IoT has been called the trend of the next internet [GBB18], highlighting the expected important role it will play in our society. IoT can be explained as, a network that consists of physical objects that are connected with sensors, software, and other technologies. This connection of physical objects is realized over the internet and focuses mainly on exchanging data [Ora20]. An IoT-based environment is therefore the whole connected environment where physical objects, operational technologies, and platforms are used to exchange data. The data generated by this environment can be combined, interpreted, and used in ways that bring a lot of benefits [Gub+13]. To Illustrate the growing relevance of IoT, in 2021 there were already over 10 billion active IoT devices. This number is expected to surpass 25.4 billion in 2030 [Jov21].

However, there are downsides to this trend. The implementation of IoT comes with major challenges and concerns. One of the major challenges that IoT encounters are the high-security risks [AR17]. In more detail, there

are millions of IoT devices that do not meet the existing security standards. This happened because the specific security challenges in IoT-based environments are not yet included in the current security assessment frameworks. As a result, governments at all levels are beginning to address the need for better IoT security governance. Two examples of these IoT regulations are relatively new: The IoT Cybersecurity Improvement Act of 2020 [Con20] and The California Privacy Rights Act [Sen18]. Because of the increasing use of IoT devices, serious security concerns, and increasing security regulations, it is essential to start properly securing IoT-based environments.

1.2 Research objective

The need to properly secure IoT-based environments is identified. Currently, this need only grows due to the rapid increase in active IoT data sources. The expansion of IoT leads to bigger environments and more communication. IoT expansion means that the universe of potential weaknesses in the environment increases significantly. In addition, bad actors only need one little weakness to exploit the environment [Del18; PwC21]. As a consequence, the growing connection of devices to the environment leads to more points of vulnerability. To overcome this growing scale of the environment, stricter communication protocols and better security surfaces are needed [GM19]. The risks of not having good security standards in place can imply that the data traffic within the environment becomes vulnerable. This risk must be minimized. In the currently available security assessment frameworks, a limited number of standards that are focusing specifically on IoT can be found [Kar+21]. Since IoT has specific characteristics it has to deal with other types of challenges than traditional computing devices. In addition, there are no security assessment frameworks that focus entirely on IoT. Therefore, the research objective is to develop a IoT specific assessment framework to secure IoT-based environments. This implies that this research will propose a assessment framework that assesses the security of an IoT-based environments.

1.3 Relevance

To the best of my knowledge, there is no existing assessment framework that is focusing purely on the security of IoT-based environments. Neither is there a framework that includes IoT as a relevant subsection to focus on in more detail. Given the rise of implemented devices and the potential of

this technology, IoT can be key in the development of our digital society. In addition, privacy and security regulations (e.g. The General Data Protection Regulation (GDPR) [Off16], The IoT-Cybersecurity Improvement Act (IoT-CIA) [Con20], and The California Privacy Rights Act (CPRA) [Sen18]) make it essential to ensure the security of data [OBr16]. In addition, the risks associated with cyberattacks are often forgotten but can have massive implications for the environment. To secure IoT-based environments to a certain level, a globally accepted framework is needed to ensure the security of the environment. The academic value that this research provides is the identification of IoT-specific threats, the proposition of solutions to these threats, and the generalization of these into a first assessment framework for IoT-based environments. This will contribute to the global journey towards optimized and secure implementations of IoT-based environments.

1.4 Research questions

A globally accepted framework is needed to assess the security of IoT-based environments. This paper's main goal is to propose such an assessment framework for IoT-based environments. As this framework must have a theoretical basis, the framework will result from the following main research question: *How to assess challenges and differences in the security of IoT-based environments, compared to the security of traditional computing devices?*

To give an elaborate answer to this main research question, the question is divided into five subquestions. Every subquestion answers a step in the process to provide the answer to the main research question with a substantial theoretical base. The five identified subquestions are the following:

- **SQ1:** *What are the limitations of the available cybersecurity assessment frameworks for IoT-based environments?*
- **SQ2:** *How can risks in IoT-based environments be assessed?*
- **SQ3:** *What are potential solutions to minimize the risks in IoT-based environments?*
- **SQ4:** *What overall process or guidelines can be implemented to improve the security of IoT-based environments?*
- **SQ5:** *How can the IoT-based environment security be generalized into an overall applicable assessment framework?*

The combination of the answers to these questions will result in an assessment framework based on substantial theory, which will propose how to assess IoT-based environments. Therefore, the main focus of this research is to deliver this conceptual assessment framework. The methodology associated with that focus is an exploratory research design, this design will be based on a qualitative research method [Cam14]. As a result, the data collected for this qualitative research will consist of interviews, existing frameworks, and literature. The combination of these data sources as answers to the research questions will form the basis for the conceptual assessment framework.

1.5 Research scope

These research questions will be answered as a part of a thesis internship at PwC NL. PwC is a company that advises businesses globally on how to improve their organization. This internship has a duration of five months and that is therefore the intended timespan for this research. The goal of this research is to be as elaborate as possible in this timespan. As this research is at PwC NL, the interviewees will be related to that organization. This means that all interviewees work for the company. These employees will work in a variety of roles and countries. This will have an impact on the diversity of the organizations that are included in this research. Therefore, the diversity in the included environments can lack in terms of type, size, revenue, and viewpoint.

As all the interviewees work at PwC, they have experience in consulting and assessing. This means that most interviewees will have a lot of experience with assessment frameworks. This makes them especially relevant to this research but also reduces the overall scope of this research. Since they will all look at the assessment framework from the view of an outsider.

Furthermore, the exact questions asked during the interview can be found in Appendix A. These questions cover the range of topics that are included in this research. The main subjects that are focused on in this research are:

- The professional expertise of the interviewee
- The most important components of cybersecurity assessment methods
- The main IoT challenges
- The methods to assess these challenges

- The scope of the framework
- The architecture of a new IoT assessment framework

1.6 Structure

To build the assessment framework, the steps above should be combined. To validate the steps taken in this research the following structure is used. This thesis consists of seven core chapters and an appendix that supports the core of this thesis. The seven chapters are listed and explained below:

1. Starting with this chapter, chapter 1, the main ideas behind the research are illustrated and the subject is introduced.
2. The upcoming chapter, chapter 2, will give a literature review on the available research within the scope of this research.
3. Thereafter, in chapter 3, the method used to generate the findings will be described in detail and substantiated.
4. Chapter 4 will present the results that are based on semi-structured interviews.
5. Chapter 5 will discuss the findings of the interviews and will stress the choices that need to be made to design the assessment framework.
6. Chapter 6 will present the assessment framework and the way to use it.
7. In the final chapter, chapter 7, the main findings and their value will be described and summarized.

Chapter 2

Literature review

The previous chapter introduced the topic this thesis is about. This chapter will elaborate on this topic and identify the most relevant concepts needed to secure IoT-based environments. Therefore, in this literature review, the current academic stance on the relevant concepts is analyzed, and these are introduced in their broad sense. However, the scope of this research triggers to mainly review the relevant topics that overlap with IoT security. In addition, since the answers to the first three subquestions are based on theory. These questions will also be discussed in this literature review. This section must include intermediate conclusions to base the subquestions on the previously identified findings. These intermediate conclusions will later be debated in the discussion and design chapter. In this section, the literature review will start with an introduction to cybersecurity. Afterward, it will identify the limitations of the available cybersecurity assessment frameworks. Thereafter, how these limitations can be assessed. And finally, what the solutions are to solve these limitations.

2.1 Cybersecurity

Starting with an introduction to cybersecurity. Unfortunately, cybersecurity lacks a consistent, agreed-upon definition [VV13; LOW15; Tro15]. However, to clarify the subject, it can be defined as "the practice of protecting critical systems and sensitive information from digital attacks" [IBM22]. Cybersecurity became relevant back in the 1970s. In 1977, the US government recognized the first security breaches in open access computer systems [Kre18]. In the period between the 1970s and now, malicious actors have found countless ways to exploit the environment. Malicious actors are users who inten-

tionally access a system with the intent to cause harm to the system or to use it in an unauthorized manner. As a reaction, the security of computer environments needed to increase significantly. In the years until 2013, securing computer environments was reactive to malicious actors. Which implies that the environments responded after an attack occurred [Col13]. However, in recent years, more proactive cybersecurity programs became mainstream [CSH15]. These programs insist on intelligence sharing and push for active detection techniques. This approach represents an opportunity for broad and collective cyber defense partnerships. Which resulted to have a positive impact on the security of computer environments. And started the current trend to proactively monitor the security risks in the organization and avoid these by treating them.

Not only malicious actors can exploit the security of the environment. Another dangerous threat that is very complicated to account for is the regular users. These users have access to the environment and possess the right credentials to make adjustments. For this reason, malicious actors may try to convince them to do something. So besides intentional malicious actors, also other users can be a huge threat. So even when the environments themselves are secure against malicious actors, malicious actors can always start attacking the environment with the help of other users that do have the authority. This can be explained using the 'weakest link' concept. The cybersecurity of an environment is only as good as the weakest link [Sch00]. Since malicious actors only need one access point to exploit the environment. In many environments, the people using the environment are the weakest link [Sch00]. Furthermore, the field in which professionals in cybersecurity are operating is changing rapidly. This is due to the fast-paced innovations in digital technologies [Bla21]. New technologies are implemented and new attacks are designed to exploit these technologies. Over time, it is essential to manage the possible risks and decrease the chances of them happening. To illustrate the current threat landscape, the top 15 most occurring cyber threats of 2020 are shown in figure 2.1.

All of these attacks are affecting the CIA triad in some way. The CIA triad is a widely used benchmark for evaluating the effectiveness of information systems security. This benchmark is based on three primary objectives of any security program: Confidentiality, Integrity and Availability [Fen08]. Confidentiality preserves authorized restrictions on information, integrity guards against improper information modification, and availability ensures the reliability to access and use of information. As mentioned before, all of the 15

Figure 2.1: *Top 15 cyber threats according to ENISA [Lel21].*

attacks in figure 2.1 exploit the lack of confidentiality, integrity, or availability of the environment. With the help of these exploitations, the malicious actors can benefit themselves in various ways. The consequences of these attacks differ for every environment, user, and device. These consequences can be minor unpleasant viruses on a personal computer but also be the cause of threats to national security. In figure 2.2 an often used illustration of the CIA benchmark is given. Where all three borders of the benchmark are just as important and necessary to protect the information within the triangle.

Figure 2.2: *CIA triad of data security [PRC18].*

Critics have evolved this benchmark due to its issues with non-repudiation. In the years after, new models came up to elaborate on the CIA triad. *The Five Pillars of Information Assurance* added authenticity and non-repudiation. Thereafter, the *Parkerian Hexad* introduced the integrity, availability, authenticity, possession or control, and utility combination. Moreover, *Information Quality* focuses on other levels: accuracy, relevance, consistency, time-

liness, and completeness. To combine all these different frameworks the *Cyber Forensic Assurance Model* (CFAM) is proposed [Dar10]. This model can be found in figure 2.3. CFAM does not only cover information security but focuses on more aspects that are relevant to forensics. Forensics is a part of cybersecurity, as it is resolving security leaks. In addition, CFAM is the most comprehensive model available and besides the CIA triad none of these frameworks is widely adopted in cybersecurity. This shows, that CIA triad has given the security a good starting point. However, the CFAM is a more complete model offering a broader scope. For this reason, this research will use the Cyber Forensic Assurance Model to assess cybersecurity.

CFA	Components
I	a) Confidentiality – ensuring that information is accessible only to those authorized to have access
	b) Possession / Control – i.e. chain of custody
II	a) Integrity/Consistency – perceived consistency of actions, values, methods, measures and principle – unchanged "is it true all of the time?" (Verification)
	b) Authenticity / Original – quality of being authentic or of established authority for truth and correctness – "best evidence" (Validity)
III	a) Availability/Timeliness – the degree to which the facts and analysis are available and relevant (valid and verifiable at a specific time)
	b) Utility/Relevance – "Is it useful / is it the right information?"
IV	a) Completeness – "Is it the whole truth?"
	b) Non-Repudiation / Accuracy – transaction cannot be denied (Validity) – no alternate hypothesis

Figure 2.3: *Model of Cyber Forensics Assurance [Dar10].*

2.1.1 Data security and protection

In the previous subsection, various ways of how malicious actors can exploit environments are discussed. This is done by illustrating the most common attacks and what important properties these attacks can exploit. The existence of a comprehensive security assessment method could minimize the threat of these attacks. However, knowing the existing threats is not enough to be secure. It is necessary to know how to prevent data from being used by

malicious actors. In this subsection, the most occurring and essential measures are discussed that are used to protect the data.

Management

First of all, the management of cybersecurity. Cybersecurity is a rapidly changing field. This implies that environments constantly need to stay on top of current developments [Bla21]. In cybersecurity, this is done through management. An important example is the education of the users. This must be monitored and managed to balance the interests. Cybersecurity management is about managing the preservation of the set of security properties in the CIA triad [Szm15]. The management process makes sure that the security is monitored and the security of the environment is continuously preserved or improved. It is the chain that makes the environment secure and keeps it secure. Management monitors the behavior of users to enforce the users to follow protocols that generate secure behavior [SSA16]. To manage all the existing domains a security management system must be comprehensive in the domains it includes. Management can use different instruments to improve the security of an environment. The ISO 27001 standard for information security management is the most commonly used and is a very comprehensive standard. The ISO 27001 includes the following domains [IEC22]:

- **Information security policies:** The organization's policies must be in line with their overall direction of information security practices.
- **Organization of information security:** The internal organization that is implemented to deal with information security.
- **Human resource security:** The secure hiring, education, and management of the users in the organization.
- **Asset management:** The security of the assets must be identified and users must know how to handle these devices securely.
- **Access control:** The access to information and information assets must be controlled. This access can be physical and logical.
- **Cryptography:** The protection of the confidentiality, authenticity, and integrity of information through encryption.
- **Physical and environmental security:** The prevention of unauthorized access to physical devices and the protection of equipment and facilities from the environment.

- **Communications and operations management:** The security of the environment's infrastructure and services. As well as the information that travels through them and the IT systems it includes.
- **System acquisition, development, and maintenance:** The security of newly purchased information systems that are included and of the existing systems that are upgraded.
- **Supplier relationships:** The security of outsourced activities performed by suppliers and partners.
- **Information security and incident management:** The process that ensures proper handling of security events.
- **Information security aspects of business continuity management:** The assurance that the information security management preserves the CIA values during disruptions of the system.
- **Compliance:** The framework to ensure that organizations comply with relevant regulatory and contractual obligations for security information.

The ISO 27001 guidelines are establishing themselves more and more as the security standard in enterprises. They provide practical guidelines for all the different domains. Guidelines that show how to implement these in management. However, not all implementations end up successful. These implementations need to be effective and efficient. Otherwise, they will not succeed [Boe08].

Education of users

The second essential security measure is the education of users. As previously mentioned, people are often the weakest link in technological environments [Sch00]. This is because most users don't completely understand computers and don't see the risks that they bring. For this reason, the first and most important thing for management to do is to educate the users about the environment. This helps to prevent the environment from attacks by malicious actors. In this education, security awareness is a fundamental requirement [McI06]. Making users aware of risks, exceptions, trustworthiness, malicious actors, and the social aspect [Sch00]. The core of education is to make the users trust the environment but also aware of threats, risks at stake, and the most common attacks. Some security applications that are often proposed to users are:

- **Backup important data and erase redundant data:** This makes sure that data will not get lost, stolen, misplaced, or corrupted. Additionally, this prevents the misuse of redundant data for malicious practices [Liu+17].
- **Patching:** Patching is the process to repair a vulnerability that is identified after the release of an environment. Therefore, it is necessary to keep computer environments up-to-date to defend against security threats [Zho+10].
- **Use strong passwords:** Weak passwords are still widespread. However, they have serious security implications [ZM09]. The authorized access to the secure environment. For that reason, the use of strong passwords is advised and often automatically enforced. Currently, passwords are often used as the main authenticator. However, better authenticators are on the rise (multi-factor authentication and biometrics [LK08; De +13]).
- **Be aware of phishing:** Phishing is an attack where the attacker creates a replica of an existing web page to retrieve important information. The information can be retrieved because the user thinks it is necessary to provide the web page with this information [CG06].

This overview shows a representation of user improvements that are currently useful. Cybersecurity is a constantly changing and developing field. This means that new securing trends come up and new attacks arise. The constant development of this field can make it hard to stay aligned with the current threats. However, security will always be essential and the education of users is key in this process. A downside to this process is that too extensive training and monitoring of users can have a negative effect. In this case, cyber fatigue can occur [RDC21]. In cyber fatigue, users are getting tired of the quantity of information. In cyber fatigue, two splitting points can be identified. Firstly, advice is distinguished from action. Secondly, attitude is distinguished from cognition. Both splits need to be analyzed to identify the case. To keep the environment secure, there must be a response to the specific cyber fatigue occurrence on all of the combinations of these points. The education of users must therefore be a balance of interests. Balancing the interests of the users with the essential cybersecurity education.

Encryption

The third essential security measure is encryption. The two sections above focus on human errors and human monitoring. However, not only human

error can lead to the exploitation of the environment. Also, optimal technological advancements must be implemented to protect the environment against malicious actors. A lot of different techniques are used to protect the environment. These techniques try to make sure the CIA triad values cannot be harmed. One of these techniques is cryptography. Cryptography resolves the problem of confidentiality, authenticity, and/or integrity by providing encryption techniques. Encryption techniques transform data in such a way that unauthorized actors cannot access the information stored in the data. This means that only authorized people know how to retrieve the information stored in the data [Dix+18]. Cryptography can be defined as the scientific study of techniques for securing digital information, transactions and distributed computations [KL20]. These encryption techniques encrypt plaintext into ciphertext (encrypted text). Different encryption algorithms vary in complexity, security, and computational need. The complexity of these algorithms is constantly increasing to oppose malicious actors since malicious actors keep finding new ways to decrypt the ciphertext. Conventionally, most algorithms make use of some kind of shared secret key as shown in figure 2.4. This key determines the exact encryption algorithm that is used to encrypt the plaintext. When only the sender and receiver know the information of this key. These two users can retrieve the information. However, this is not possible for the malicious actors.

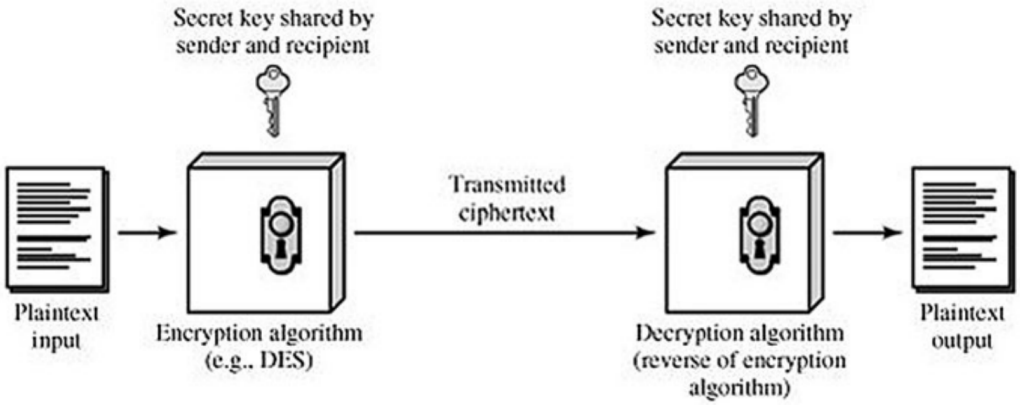

Figure 2.4: *Conventional encryption [Dix+18].*

In the example of figure 2.4, an example of Encryption in Transit (EIT) is shown. Data can occur in various states: data at rest, data in motion, and data at use [Fit19]. All three states need to be considered and secured extensively. In the case of EIT is looked at data in motion. This means that the data is encrypted that moves from one point to another [SD11]. In this transition,

the whole process is considered to be secure. Therefore, it is only fair to say that the transition is safe whenever the data is encrypted before it leaves the computer and decrypted after it arrived at the computer of the receiver. This phenomenon is called end-to-end encryption. In the current digital world, protocols like SSL, TLS, and HTTPS are implemented to widely accommodate end-to-end encryption [Ran+16].

Another important source that needs to be secure is Encryption At Rest (EAR). This takes care of data at rest and makes sure that all the data that is stored is encrypted to oppose malicious actors. In this way, malicious actors are not able to retrieve information from the data [SD11]. This process is similar to the situation illustrated in figure 2.4. However, in this case, the ciphertext is transmitted into the database. And after the sender wants to retrieve the data again, it is decrypted.

Besides the previously indicated difficulties cryptography faces concerning innovation, there are also other struggles. First of all, the third state of data: data at use. Data cannot be used while it is encrypted. Therefore the security issues on the use of data stay and cannot be solved using encrypting. Second of all, the complexity of encryption algorithms is increasing. This leads to increases in computational costs. As a result of rising computational costs devices that have limited computational power or energy are jeopardized. To solve this second problem, lightweight encryption algorithms are being developed and can be implemented for these devices [RH11].

Intrusion detection

The fourth essential security measure is intrusion detection. Although organizations can implement different preventive measures to reduce the risk of a successful attack, it is not possible to completely mitigate all risks involved for an organization. For that reason, it is important not to only implement preventive measures, but also detective measures, often referred to as intrusion detection. Intrusion detection should protect against all the objectives in the CFAM model. To detect intrusion it can include the following capabilities [AG11]:

- It monitors and analyzes both the user and the system activities
- It analyzes the systems configurations and vulnerabilities
- It assesses the system and the file integrity

- It recognizes attacking patterns
- It analyses abnormal activity patterns
- It tracks user policy violations

In intrusion detection research, different studies focus on an important subcategory of detection. This focus is specifically on malware detection. Malware is short for malicious software and is a widespread term. It encompasses malicious activity such as viruses, trojans, spyware and other intrusive code [VY06]. As malware can take different forms, all six capabilities stated above could be used to detect certain types of malware. So when an Intrusion Detection System (IDS) works properly it should detect the malware. However, as attackers get more sophisticated, malware is getting harder to detect. Malware can be detected in various ways. A behavior-based detection algorithm currently scores best with a malware detection rate of 96%. However, this 4% margin of undetected malware is too much in terms of security [AS20]. The lack of accuracy could be explained by the limited amount of available benchmark datasets [Sha+20]. Therefore, to optimize the malware detection more research and more elaborate datasets are needed.

The broader category called intrusion detection detects all malign intrusions over the computer network and devices. Therefore, these detect policy violations and malicious activity. Most of these intrusions are used to identify and scan the vulnerabilities of a network or computer system [Sha+20]. When detecting we cannot forget about the attacks that are not covered by malware detection. These attacks need another kind of detection method. However, despite enormous efforts by different researchers [Lia+13; Vin+19], intrusion detection systems are still struggling to improve detection accuracy while reducing false alarm rates in detecting novel intrusions [Ahm+21]. This concludes that intrusion detection methods add a lot of security to the environment. They are becoming more and more secure and detect a lot of malicious codes. Nevertheless, these methods are not perfect. Therefore, malicious use can still appear undetected. For optimal security, the need to improve these detection methods stays.

Security tools

The last essential security measure are security tools. Managing cybersecurity is not always needed from scratch. A lot of tooling and software are de-

signed to tackle individual problems. A selection of security ensuring tools that exist is:

- **Firewall:** Provides security to companies that are online on the internet and it protects their network sites against external attacks and intrusion [LL00].
- **Anti-virus:** Provides software that uses a virus signature to find a specific virus in a computer file system. It detects, quarantines, and removes the virus. This software needs to update frequently to be able to detect new signatures [WJ18].
- **TLS:** Runs on top of TCP/IP to make sure the different OSI layers are secure [Par+06; Sin+17].
- **VPN:** Provides secure communication between a set of sites and a close user group. They are most valuable as a provider of security on insecure networks. Besides, compared to other secure options VPNs have the advantage of being cheap and scalable [Zha+04].
- **Anti-spyware:** Monitors attacks, identifies the malicious spyware, and removes it from the system. Spyware is a specific security threat that monitors a user's activities, creating serious security issues [LK08].
- **Authentication tools:** Provides secure authentication. With the help of multi-factor authentication, such as biometrics (fingerprints, unique personal characteristics). Authentication is getting more secure. However, the computational costs are also increasing in comparison with traditional means of authentication such as passwords [De +13; Kre18].

These tools provide more security to environments, whenever they are implemented and used right. In every individual case, the possibilities and necessities must be analyzed. A lot of different approaches are possible for malicious actors. However, there are also a lot of possibilities to secure the environment. Essential is to stay up-to-date, to oppose new types of attacks [Zho+10].

2.2 Current limitations of assessment frameworks

As the previous section described, the implementation of a secure environment is elaborate and complex. To guide organizations through this process

cybersecurity assessment frameworks have been developed to assess the implementation of these environments. However, the currently available assessment frameworks often do not account for the challenges in IoT-based environments. Therefore, it is essential to get an answer to subquestion 1. This question will be discussed in the coming section. The question is formulated as follows: *"What are the limitations of the available cybersecurity assessment frameworks for IoT-based environments?"*

2.2.1 Current available frameworks

The literature about cybersecurity assessment frameworks contains a wide range of articles. The available literature is very elaborate and varies between articles that evaluate a model, model a framework, or give a general overview. This subsection will include the theories and methods that are currently the most relevant. Furthermore, these articles can focus on different subcategories of the overall assessment method. In literature, the most researched subcategories are:

- **Quantitative metrics:** Make security values measurable by defining objective measures, questions, and splitting points [HC13].
- **Cybersecurity risk assessment:** Identify the threats, vulnerabilities, consequences, and likelihoods that are associated with the environment [Gan+20].
- **Security standards:** The set of standard rules that should be followed in order to provide secure properties. These standards function as minimal requirements for everything included in the environment, like the ISO/IEC standards [IEC22].
- **Cybersecurity regulations:** The legal privacy and security values that must be followed in order to meet governmental regulations. The regulations are very context specific and can depend on the region the environment operates in, like the GDPR, IoT-CIA and CPRA [Off16; Con20; Sen18].
- **Cybersecurity assurance:** Perfectly securing the environment is only possible when security is assured. In some cases this assurance can be achieved by combining management reviews, cyber risk assessments and cybersecurity controls audits [Sab+17].
- **Cybersecurity maturity:** Identify the level of cybersecurity maturity of an organization [Pau+93; Ali+20; MSB21].

- **Cybersecurity management:** Manage the preservation of the set of security properties in the CIA triad [Szm15].
- **Generic cybersecurity assessment:** Combine all different subcategories into one generic cybersecurity assessment framework [Kar+21].

As the last point states, all these subcategories need to be combined to provide an assessment framework. Since the quantitative metrics are a subcategory of the other parts, they are not included in an architecture. In addition, cybersecurity assurance is a sub-part of the overall maturity of the environment. Therefore, this would mean that when the architecture shown in figure 2.5 would be created, this would cover the most important components of an assessment framework.

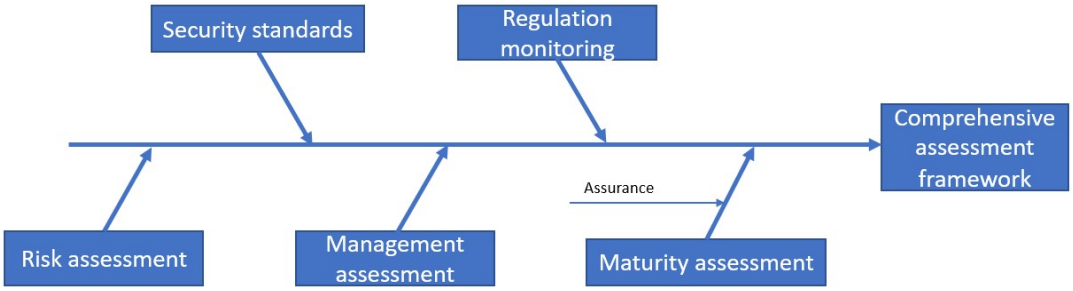

Figure 2.5: *Fishbone diagram of the architecture of an assessment framework.*

The number of articles on these topics is large. This amount is unfortunately too excessive to be covered in this research. Therefore, another research that summarized the most relevant articles is used as a baseline. This research recently studied the relevant articles on security standards and assessment frameworks [Kar+21]. The overlap of relevant articles with this research makes that they have already identified the majority of the relevant articles for this research. Besides security standards and assessment frameworks, the baseline included NIST special publication on security techniques. In this case, the use of a baseline article means that the main findings of this article will be used as the main explorative to base further research on. The conclusions will be further investigated, adjusted, and expanded whenever necessary. The baseline reviews the IoT abilities of 37 different security frameworks. These include 7 NIST special publications on security techniques. In addition, it discusses 80 ISO/IEC security standards and 32 ETSI standards. Since the baseline article does not include all mentioned subcategories, these are added to broaden the view.

The additional frameworks that are added must have the premise that they follow from recent research and include a relevant contribution to the baseline. The additional articles will be stated in the remainder of this subsection. Starting with a critical article, Leszczyna states that the application of most frameworks is not tested or reviewed [Les21]. This jeopardizes the quality of these frameworks since there is no assurance that they are applicable. Research that did provide a framework that chose to focus on applicability is called the Cybersecurity Focus Area Maturity (CYSFAM) Model [OLS21]. CYSFAM is an extension of the information security Focus Area Maturity model [SR14]. CYSFAM made self-testing critical to its assessment. The benefit of making self-testing essential is that there is little space for subjectivity in the assessment model because the assessment will be objective. Therefore, a model should strive to eliminate subjectivity. The maximal elimination of subjectivity can be achieved by good regulation of quantitative metrics. In addition, models that have explained how they have made their quantitative metrics objective are also available. An example is The Three Tenets Model of Cybersecurity [HC13]. This model formed a base for the quantitative metrics that were used in later research [WH16; Iwa21]. These researches imply the importance of reviewing the assessment methods, preferably with the help of an self-assessment method. Focusing on the included quantitative metrics.

Additionally, another overview of existing assessment approaches is created in recent research [Lia+21]. This recent research was not yet available to the baseline. Since the baseline was only able to retrieve methods created before it was published. In addition to the approaches in the baseline, the new and relevant models that are created will be included in the baseline to broaden the view. First of all, a Maturity Model for IoT Adoption is created [KS22]. Secondly, cybersecurity models for secure IoT implementation are identified [Ech+21; DB21]. In addition, research is done on the security architecture of IoT implementations [BR+21]. Moreover, in regulatory scope, the GDPR was the only one included in the baseline. However, also the IoT-CIA and CPRA are relevant to consider in this research [Con20; Sen18]. Furthermore, more research is done on the cybersecurity assurance of IoT-based environments [Cha+21]. Lastly, new ISO/IEC and ETSI are out and need to be considered.

All these new researches focus on their subcategory and have introduced IoT topics in their model. Therefore, the already available researches for the baseline need to be combined with the newly introduced models. To

create a comprehensive framework that covers all aspects of IoT-based environments, every subcategory needs to be included in an overall assessment method. This is essential since security is just as good as its weakest link. The neglection of subcategories will result in the presence of the weakest link. In addition, in these models self-assessment must be striven for to make the model applicable. This can be achieved by eliminating subjectivity in the quantitative metrics.

2.2.2 IoT specific risks

In addition to the analysis of the existing frameworks, it is essential to identify the risks that are specifically relevant to IoT-based environments. IoT-based environments have certain characteristics that make it another type of target than traditional computing devices. Starting with the capacity concerns, the Internet of Things consists mostly of devices with limited resources. As a consequence, most IoT devices have low computational power, small storage space, limited battery capacity, and low bandwidth [BSE18]. So compared to traditional computing devices the design of IoT devices must make a difficult consideration. Besides, all IoT devices in the environments must meet specific characteristics. Some of these make them specifically vulnerable to certain threats. These will be discussed in the coming subsection. In addition, in a lot of cases, the main focus of designers is to make the devices work. Not necessarily to make them perfectly secure [Kar+21]. In combination, this subsection will elaborate on the characteristics of IoT-based environments and illustrate what security implications these have. Starting with the fundamental characteristics of IoT-based environments and their corresponding security implications [PP+16]:

- **Interconnectivity:** All IoT devices in the environment can be interconnected with other devices and with the internet. This has the security implication that the exploitation of one device can bring harm to all devices that are connected over the same network [Kar+21].

- **Things-related services:** The IoT device is capable to provide the service that it was originally made to do. This limits the devices to optimally use technological possibilities. Impacting the security of the device [PP+16].

- **Heterogeneity:** The most IoT devices are heterogeneous, which means that different devices are based on different hardware platforms and/or

different software. The lack of standardization makes it harder to generate standards and protocols for these devices. This makes it more complex to secure the environment [Kar+21].

- **Dynamic changes:** The state of devices can change (on/off), these states change the size and dynamics of the whole environment. Securing a dynamic environment is more complex than securing a static network [PP+16].
- **Enormous scale:** The total number of devices that are connected to an environment is increasing significantly compared to traditional computing devices. One of the main security implications is the extreme growth of the attacking surface, with more devices and more data traffic to attack [Kre18].
- **Connectivity:** All devices need to be connected to the environment and can produce/consume data. This is the minimum capability that a device needs to have to be called an IoT device. However, also makes every IoT device a target since it contains relevant data [Kar+21].

All of these characteristics have security implications for IoT-based environments. Therefore, providing a secure environment is more complex for IoT than for traditional computing devices. This means that it is essential to identify the implications and generate secure processes that solve these implications. This is essential to be able to implement a secure environment. Besides the fundamental characteristics of IoT devices, IoT-based environments also have a standard architecture. This architecture can be split up into multiple layers. How these layers are called and where the splitting point is between these layers varies. However, apart from the implemented security protocols these architectures will mostly be similar [PP+16; CV+15; VZS10]. A visual indication of the architecture is given in figure 2.6.

In this example, four layers are identified in the IoT architecture. These include an sensing, network, service, and interface layer. These layers present the communication between different IoT devices, what steps are needed to provide for this communication, and with what type of communication the data is shared. Some often occurring IoT challenges can be found when this standardized IoT-based environment architecture is analyzed. Therefore, the main risks and disadvantages associated with IoT architectures are identified [CV+15]. The architecture layer, risk level, and corresponding disadvantages can be found in figure 2.7.

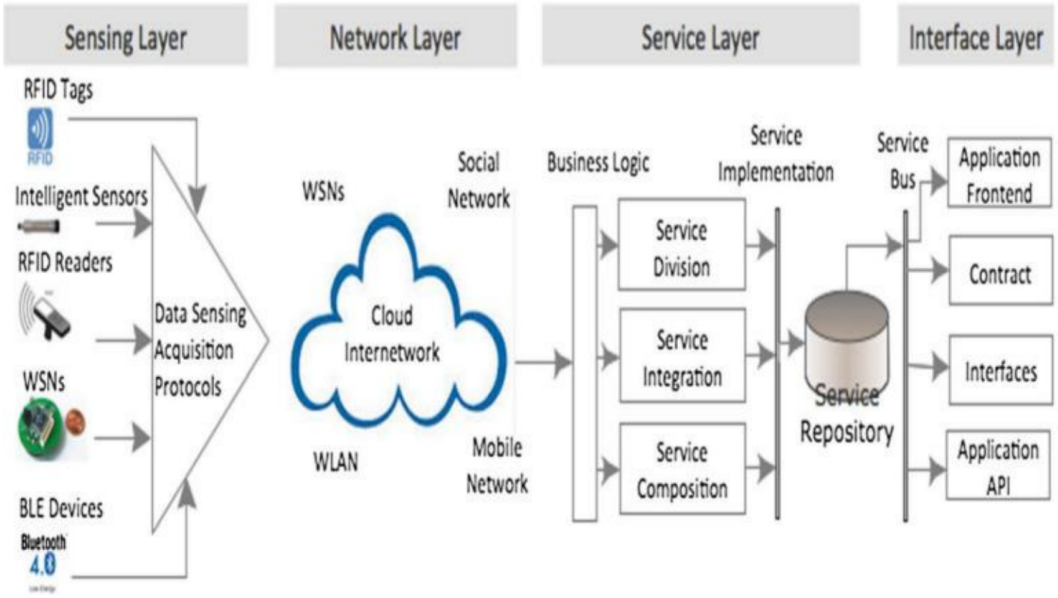

Figure 2.6: *Architectural Layers of IoT [VZS10].*

The device characteristics and the architecture of IoT-based environments are discussed above. However, this is not everything that makes IoT vulnerable. Another issue is that IoT is especially vulnerable to regulatory changes currently. New technological trends and the implementations of these trends come with an increase in importance and impact in our society. The rise of these technologies will always increase the amount of political interest, the number of laws, and the number of regulations associated with these technologies [Kar+21]. In this case, regulators will have to decide on what will be called secure and what rules IoT-based environments must meet. These rules probably have an impact on the whole architecture of the environment and force boundaries on the devices. However, the main objective of these rules will be to optimize security in these environments. Therefore, it can be assumed that whenever an IoT-based environment is optimally secured, it will meet most regulations. Recently, also the regulatory risks of IoT adoption have been identified [BJH20], the results of this research can be found in figure 2.8.

Until this point, only abstract risks have been identified. However, the possible attacks and exploitations of the IoT-based environments have not yet been identified. To emphasize the importance of a secure environment a list of common consequences is presented. This is based upon the list of Karie et al. who have identified a list of security and privacy concerns that

Layer		Risk level	Disadvantages	Description
Perception		High	Physical characteristics of devices	Small dimensions require installation of hardware with even smaller dimensions and limited possibilities
			Price of device unit	The low price of the device results in the implementation of low-cost components of limited possibilities
			Physical exposure	Great number of devices located in the real environment is often difficult to protect against physical impact and an unauthorized manipulation
			Energy requirements	Devices have to satisfy high demands which results in the implementation of energy-saving components of limited possibilities
			Wireless communication	The use of the air as a data transmission medium allows unauthorized and simple data collection and the analysis of traffic that is often unencrypted or, because of the limited hardware capabilities, encrypted using weak cryptographic methods
			Implementation of security methods	Previously mentioned restrictions prevent the implementation of more robust methods of protection applicable to traditional information and communication environments
			Heterogeneity	A large number of devices using different transmission technology make it difficult to establish standard protocols and protection methods
Network	Access sublayer	Low-to-Medium	Application of the wireless communication technologies	The use of the air as a data transmission medium allows unauthorized and simple data collection and the traffic analysis
			Convergence of multiple users / devices at a single point	Due to connection of multiple devices in a single point (switch / hub), that point may be exploited for the implementation of a large number of attacks (eavesdropping, MitM, DoS, etc.).
	Internet sublayer	Low	Routing	OSPF, BGP, and other routing algorithms have flaws that can be exploited for the purpose of security breach
			Publicly exposed routers	May be the target of the attacks such as DDoS
Middleware		Medium	High penetration in the number of users	One cloud computing service provider manages the data of a large number of private and business users which raises the issue of data segmentation, privacy, confidentiality, and similar.
			Low level of maturity of the technology	The rapid development of services based on cloud computing in recent years raises the risk due to insufficient research and the lack of protection methods
			Ability to set a large number of users classes on a single physical machine	Identified vulnerabilities of virtualization whose exploitment can causesimultaneously damage to a large number of users

Figure 2.7: *Risk classification of the IoT architecture layers [PP+16].*

IoT-based environments need to consider [Kar+21]. Important concerns they identified about security are Data and Information Leakage, Identity theft, Denial of Service (DoS/DDoS), Health and Safety of Users, Eavesdropping, and Software Exploitation. The consequences of these attacks can be of varying scales depending on the included data and the target. The identified security concerns are very much aligned with the most occurring cyber threats according to ENISA, which were illustrated in figure 2.1. In addition, the most important concerns about privacy that they identified are Data Storage and Usage, Tracking and Location Privacy, Context-Aware or Situational Privacy, and User Privacy Information Mining [Kar+21]. Also in this case, the consequences of these attacks can be of varying scale depending on the included data and the target.

To correctly validate IoT-based environments, these IoT-specific concerns

Synthesis of potential risks generated by IoT adoption in organizations.

BOLD aspect	Unexpected Changes Caused by IoT Adoption	Resulting Organizational Risks
Big	Changes to laws and public opinion means that organizations need to be aware of potential disclosure of individual data which could reveal sensitive information such as personal habits or personal financial information.	Data privacy conflicts resulting in reputational damage and possible legal action. Changes in accuracy of data on which decisions are made.
	High development and implementation costs are important impediments to the implementation and application of IoT often results in unforeseen expenditure.	High implementation costs can result in unexpected, added pressure on tight budgets.
	Limitations in information technology (IT) infrastructural capabilities and data management with regards to increasing volumes and speeds of data delivery mean that structural changes to the IT infrastructure of organizations are often required.	Difficult interoperability and integration mean that architecture, energy efficiency, security, protocols and quality of service can be affected by IoT adoption.
Open	Technological and regulatory challenges regarding data sharing and data protection often need to be addressed during IoT adoption.	Data security breaches and data leaks leading to reputational damage, potential loss of intellectual property and lost production.
	Sophisticated mechanisms to publish and share things and ways to find and access those things often need to be developed.	The need for solutions for providing fine grained access control need to be developed restricts organizations in their ability to share data responsibly with the right people at the right time.
	A lack of standard IoT architectures and missing chains in IoT research and development means that organizations often need to develop their own architectures and technologies which, in turn can impact the market	Conflicting market forces of supply and demand mean that organizations often need to develop their own research and development regarding IoT, often in cases where IoT is not their core business. However, a lack of sufficient knowledge regarding IoT can inhibit this development.
Linked	Policies and regulations regarding IoT and the linking of data and things often need to be developed.	Lack of sufficient legal frameworks mean that organizations are often exposed to either over-linkage leading to security or privacy issues, or take unnecessary steps to prevent linkage, reducing the level of benefits.
	A lack of acceptance of IoT means that organizations often need to develop trust in the new systems. The greater the trust of users in the IoT, the greater their confidence in the system and the more willing they will be to participate.	Lack of trust in IoT means that implemented systems are often not fully exploited resulting in a reduction of benefits.
	The heterogeneity traits of the overall IoT system make the design of a unifying framework and the communication protocols a very challenging task, especially with devices with different levels of capabilities.	Linking heterogeneous data from heterogeneous data sources can create data quality issues resulting in misleading information.

Figure 2.8: *Synthesis of potential risks generated by IoT adoption in organizations [BJH20].*

and risks must be covered in the assessment framework. Therefore, it must cover IoT-specific challenges, IoT architecture-specific challenges, regulation uncertainty, and account for security and privacy concerns. For these reasons, the following subsection will elaborate on how these can or can't be found in current frameworks.

2.2.3 IoT-based limitations of these frameworks

In the subsections above, the main characteristics of IoT-based environments have been stressed. These characteristics should be covered by cybersecurity assessment frameworks for IoT-based environments. This subsection will discuss what these assessment frameworks cover. Thereafter, the current assessment frameworks are tested on these characteristics. Finally, the outcomes of these tests are discussed to identify the IoT limitations of the available cybersecurity assessment frameworks.

Starting with a summary of what an assessment should cover to properly assess IoT-based environments. At first, there are eight essential values that all environments and all devices in these environments must meet to be secure (CFAM). These values are: confidentiality, possession, integrity, authenticity, availability, utility, completeness, and non-repudiation [Dar10]. These eight values must be applied to all levels of the IoT-based environ-

ment. Secondly, to ensure and test these values assessment frameworks have been created. These frameworks often assess a subcategory of the whole cybersecurity field. These subcategories are the most important topics in the literature. By putting them all together, a comprehensive framework should be generated. These subcategories are risk assessments, security standards, regulations, maturity assessments, and cybersecurity management. Thirdly, it is essential to these assessment methods that they are applicable in real-life examples [Les21]. This can be achieved when striving for objective self-assessment. The main goal of these assessment frameworks is to provide relevant outcomes to an environment. Therefore, whenever an assessment framework is used it should have generated relevant outcomes for the assessed environment.

The characteristics of IoT devices and IoT-based environments, make IoT especially vulnerable. The interconnectivity, things-related services, heterogeneity, dynamic changes, enormous scale, and connectivity all make the security of IoT-based environments more complex. In addition, the IoT architecture layers face a list of risks that are illustrated in figure 2.7. Together with the security concerns that are identified by Karie et al., an elaborate overview of the vulnerabilities of IoT-based environments is generated. The baseline identified the following main challenges for the current IoT security assessment frameworks [Kar+21]:

- **Technical challenges:** Are the challenges that must be solved by technical experts. They are easy to identify and define and their solution is based on experts' knowledge and skills. Examples are computational power, costs of the product, secure wireless communication, energy efficiency, cryptography, and architecture.

- **Legal challenges:** Are the challenges that are related to legal regulations and can include both civil and criminal aspects. Do not only affect malicious actors but can also specify how service providers use, store and secure users' personal information. E.g. privacy, discrimination, and accountability.

- **Ethical challenges:** Are the challenges that present people with tough choices of what is good or bad, what is acceptable or not. E.g. data and information integrity and trust.

- **Operational challenges:** Are those challenges that could create waste, drain resources, impact operational performance, render a business

less profitable and hinder devices in the environment that are not implemented correctly. E.g. physical access, heterogeneity of devices, uneducated employees, vagueness, and management.

- **Adaptive challenges:** Are complex, ambiguous unpredictable, volatile, fluid challenges that change with circumstances. It is hard to identify a solution since there are no solutions available or too many options. E.g. in-house knowledge, user expectations, and cultural changes.

These five challenges are presented as critical to IoT assessment methods. However, in none of the articles they can be identified simultaneously. For that reason, the baseline criticizes the selected articles. In this research, we address these five main challenges. These are combined with the earlier findings that are found to assess the other assessment frameworks.

Firstly, the maturity models are discussed. Starting with the Cybersecurity Focus Area Maturity (CYSFAM) Model [OLS21]. These researchers focused on the applicability of the model and implemented this with the help of a self-testing model. They covered the five challenges of [Kar+21]. However, they mainly issued the challenges on a high level. Besides, it was not designed explicitly towards IoT devices. Therefore, it neglects the quantitative metrics for IoT-based environments. In addition, the model would have been considered applicable when clear definitions of the areas would have been given. The second maturity model is the Maturity Model for IoT Adoption [KS22]. This model discusses the importance of strategic IoT implementation. However, on security challenges, it is not able to offer solutions besides the implementation of the NIST framework.

Secondly, besides the baseline, another overview of the existing IoT assessment approaches is proposed [Lia+21]. Also, this overview does not identify a real model. However, this overview identifies a list of IoT security features. This list is useful to access the security that it covers. Nevertheless, it fails to identify important parts of the adaptive and operational challenges. As there is no place for user training and cybersecurity management. For this reason, also this overview is not able to propose a comprehensive overview.

Thirdly, cybersecurity models for secure IoT implementations are discussed. Starting with a Cybersecurity Model Based on Hardening for Secure IoT Implementation [Ech+21]. This model has used a case study to show its applicability. Furthermore, it has a wide range of security levels and covers most of the challenges. However, the study focuses solely on the implementation of the environment. This means that it fails to identify the adaptability

of the environment and the management of the environment. This will result in an implementation that will provides a lot of security. However, the implementation will not be able to provide continuous security. In addition to this model, three other kinds of research have been done on improving the security of IoT implementations. These are the following researches. *Securing IoT devices using zero trust and blockchain*, *Security trends in IoT: a survey*, and *Towards assurance and trust for the IoT* [DB21; BR+21; Cha+21]. The results of these three articles provide clear solutions and improvements for the security of IoT devices. Nevertheless, also these articles are not able to give a comprehensive framework. Individually all articles are neglecting legal, ethical, adaptive, and operational challenges.

Lastly, new ISO/IEC and ETSI standards are out and new regulations were introduced. The critique on the ISO/IEC and ETSI standards in the baseline was that not enough security standards and assessment frameworks were designed to directly address the security needs of IoT-based environments [Kar+21]. New standards have not changed this amount, and therefore the same critique is relevant to these new standards. In addition, the new regulations IoT-CIA and the CPRA require IoT cybersecurity to increase [Con20; Sen18]. In California, they have already standardized password hygiene, multi-factor authentication, and VPNs.

2.2.4 IoT limitations of cybersecurity assessment frameworks

Concluding, this section aims to answer subquestion 1. Formulated as: *"What are the limitations of the available cybersecurity assessment frameworks for IoT-based environments?"* To answer this question, the available cybersecurity assessment frameworks were discussed. Followed by the characteristics and challenges of IoT. And finally, the framework mismatches to the IoT implementations were identified. The following sections will be based on the results found in this section. Therefore, the first intermediate conclusion of this research, which is also the answer to subquestion 1 can be summarized as follows:

- **Comprehensiveness overall framework:** The assessment framework must cover all levels of the assessment. Important components here are risk assessment, security standards, management assessment, cybersecurity regulation, and maturity assessment.
- **Comprehensiveness assessment method:** Every assessment method must have the goal to provide relevant outcomes. Examples of this

are educational needs, managerial improvements, protection improvements, detection methods, and providing available software to increase the security of the environment.

- **Major challenges for current IoT security frameworks:** The major challenges for most assessment methods are to contain and assess the following five challenges: technical-, legal-, ethical-, operational-, and adaptive challenges.

- **Applicability of the framework:** The applicability of the framework is often neglected. However, the framework cannot be successful, if it is not applicable nor shown how to be applied.

2.3 Risk assessment in IoT-based environments

In the previous section, the limitations of the available cybersecurity assessment frameworks for IoT-based environments have been identified. However, the goal is to create a comprehensive assessment framework. Therefore, it is essential to know how to assess these limitations. The assessment of these limitations is done by answering subquestion 2. This question is formulated as follows: *"How can risks in IoT-based environments be assessed?"*

2.3.1 Risk assessment methods

The assessment of IoT-specific problems is similar to other IT problems. The only difference is the topic. Therefore, IoT-specific risk assessments focus on other characteristics. According to NIST, a risk assessment is "the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur" [SN12]. NIST identifies the threats, the vulnerabilities, the impact, and the likelihood that are associated with the risks. According to Ganin et al., threats, vulnerabilities, and consequences are the most important aspects of this definition. They discuss the hierarchy between these three in the risk assessment [Gan+20]. To emphasize the relation between these domains, a multicriteria decision framework for cybersecurity risk assessment and management is created. The visual representation of it can be found in figure 2.9.

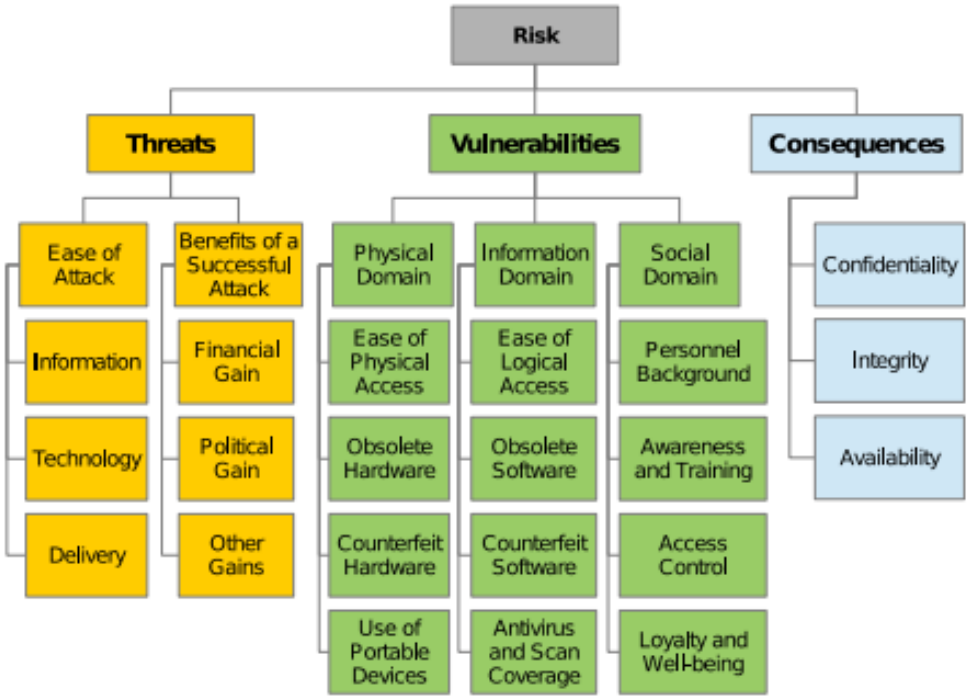

Figure 2.9: *Hierarchy of the Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management [Gan+20].*

The framework splits risk assessment into the three domains (threats, vulnerabilities, and consequences). It identifies these domains and relates specific criteria relevant to that domain. In the framework, the consequences have been identified as the values in the CIA triad. However, as stated in the cybersecurity section, in this research the CFAM model is preferred over the CIA values. Since the CFAM is a more comprehensive model than CIA, also including non-repudiation.

As vulnerabilities, the model chose to classify three out of four domains of DiMase et al., combining the social and the cognitive domain [DiM+15]. Other research has identified two domains, also combining the physical and social domain [AH19]. This research identified the assessment methods that are relevant in every domain. To stay aligned with the model, these assessment methods are presented in three different domains.

- **Physical domain:** Hardware threats assessment method, policy & countermeasure assessment method, and natural threats assessment method.
- **Information domain:** Vulnerability assessment method, network as-

sessment method, virus detection assessment method, authentication assessment method, and penetration testing assessment method.

- **Social domain:** Human assessment method.

To identify all the vulnerabilities, all of these assessment methods should be implemented. For threats, the model is based on the work of Mateski et al. This work proposed a clear overview of the relevant topics [Mat+12]. The framework fails to identify the likelihood, this was a substantial part of the definition by NIST. A good practice to determine the likelihood of IoT risks through risk likelihood parameters is proposed in the work of Kandasamy et al. [Kan+20]. In addition, NIST stated that a modern IoT risk assessment method cannot be a one-time assessment. It should be a repeatable process [SN12]. A visual representation of how the NIST method focused on a repeatable process is illustrated in figure 2.10.

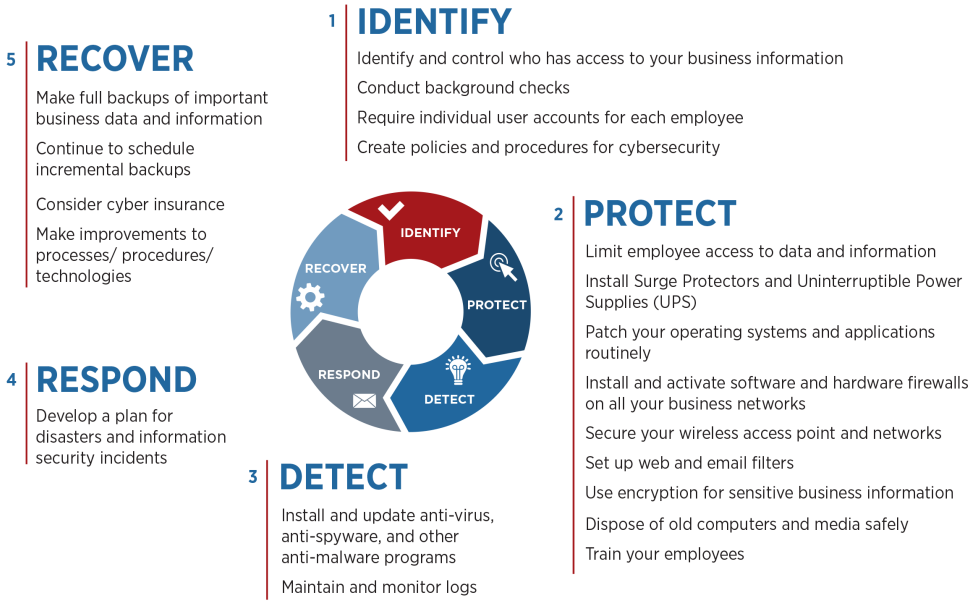

Figure 2.10: *NIST cybersecurity assessment framework [SN12].*

The NIST framework is currently one of the most used frameworks. It identifies multiple steps in the process of fixing security vulnerabilities. All these steps have their impact on the threats and consequences. For example, when a model is assessed, it is relevant to know how easy it is to respond to an attack but also to know how easy this attack can be detected. Only the

five topics together can fully identify the security impact. Therefore, at every security vulnerability, these five steps need to be evaluated to create a clear assessment of the risk.

In later research, Lee focused on another important topic in security assessments [Lee21]. He created the cyber investment cost analysis which focuses on the financial aspect of security risks. It identifies the financial consideration of securing the environment. It tries to identify the optimal financial choice, and to what extent it is financially optimal to secure the environment. In this research, this choice is based on perfect knowledge of the financial costs when attacked, the probability of security, and the costs related to reaching that probability. However, one of the biggest barriers in IT projects is the difficulty of measuring the benefits and costs of cybersecurity risk management. Therefore, the realization of perfect information is rarely the case. However, it gives a good illustration of the importance of good security. A visual illustration of the analysis is given to show the relationship between financial costs and the cyber investment costs in figure 2.11.

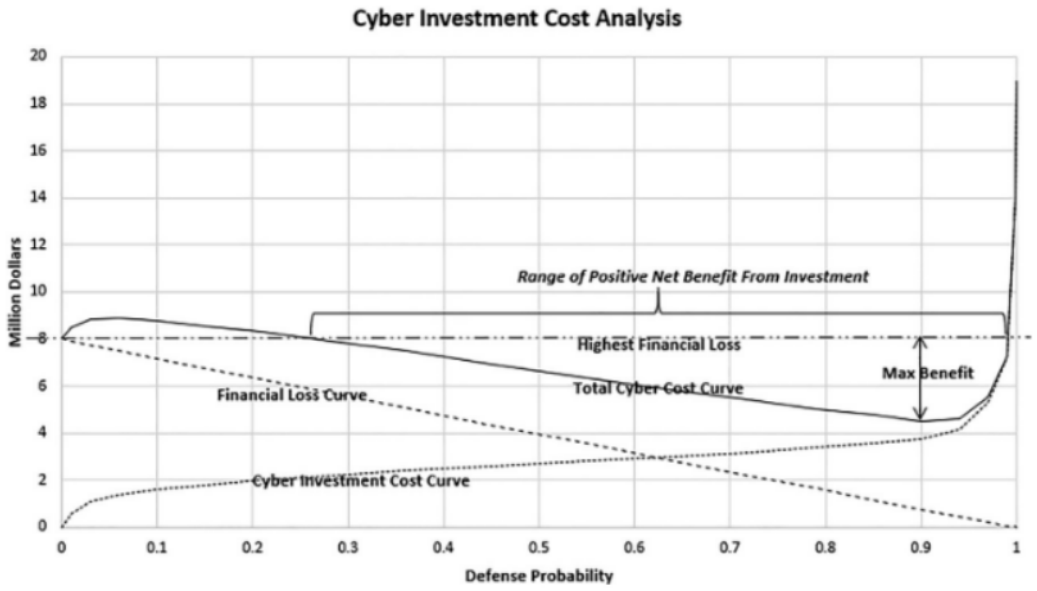

Figure 2.11: *Cyberinvestment cost analysis [Lee21].*

This subsection has identified the hierarchy between different threats, vulnerabilities, consequences, and their likeliness. This is extended with the available assessment methods on these topics. Additionally, the different steps in the assessment of a security vulnerabilities are identified and the

cyber investment cost analysis is discussed.

2.3.2 Risk assessment limitations

In the previous subsection, multiple assessment methods have been identified. In this subsection, the limitations of these methods for the IoT-based environments challenges are discussed. Earlier, the limitations of current assessment methods have been identified. These limitations were concluded to be the following:

- **Comprehensiveness overall framework:** The assessment framework must cover all levels of the assessment.
- **Comprehensiveness assessment method:** Every assessment method must give all the relevant outcomes.
- **Major challenges for current IoT security frameworks:** The five major challenges: technical-, legal-, ethical-, operational-, and adaptive challenges.
- **Applicability of the framework:** The applicability of the framework is often neglected. However, this is crucial for the success of a framework.

For the first two points, the assessment framework just needs to fit the boxes. Checking the frameworks and their sub-frameworks to be comprehensive. However, the five major challenges in IoT security do need to be identified in more dept. Besides, testing the applicability of the framework can be complicated.

First, the five major challenges identified by Karie et al. need to be discussed to show how these can be assessed [Kar+21]. Therefore, it is necessary to conceptualize the challenges into real problems. Research has been done on where current risk assessment methods fail, focusing on IoT [NCD17; Nur+18]. The four key failures that are identified and need to be secured are discussed below.

The first key finding of the research by Nurse et al. is that assessment frameworks structurally fail to recognize that items cannot always be an asset if they are not secure [NCD17; Nur+18]. In current assessment methods, devices are often valued as assets and forgotten to be valued as an attacking platform for malicious actors. This attacking platform is strengthened by the second key finding. Which looks at the organizational structure of the

environment. In the situation that someone can predict how the layers are connected and how the environment is organized. Then it is also possible to exploit the environment. This can happen across all different dimensions of the environment. Thirdly, the periodic assessment was already a vulnerability for older environments. This is only getting more exacerbated due to the rapidly changing dynamics of IoT. Currently, risk assessments are focusing on existing risks to the environment. This will not be sufficient for IoT because these environments change shape quicker than the assessments can account for. Therefore, assessments need to account for future developments in the environments and act upon them. Lastly, there is a growing lack of internal knowledge about IoT-based environments. This lack of knowledge is greatly impacting the security risk assessment. Currently, most assessment methods try to be self-assessing to make it available to everyone. However, if the environment is internally not well understood, it cannot be assessed properly.

These four key findings illustrate how the main 5 main challenges are not covered by the current assessment frameworks. Therefore, future assessment frameworks must account for these four failures. This means that it is necessary to act upon them and offer solutions to them to create secure environments. Additionally, the failure to cover IoT in the assessment methods also means that they do not cover the risk mitigation of IoT. This is relevant to minimize the impact of cyber risk. When environments expand quickly and retrieve a lot of data it is essential to mitigate the potential risks. A useful model that all IoT devices should follow to mitigate the risks is the three tenet model [HC13]. The three identified tenets are:

- **System Susceptibility Metric:** Minimize the number of access points to system-critical functions, these can be functionalities and services.
- **Access Point Metric:** Minimize the number of visibility to a malicious actor, this can be input/output values and system processes.
- **Threat Capability Metric:** Minimize useful insight available to the malicious actor, for example system operations where data observed at one time may or may not be comparable to data observed at another time or on another system.

Second, the applicability of the model must be tested. Current frameworks are often not properly tested on their applicability. Therefore, a good method is needed to self-assess the applicability of the created framework. A method to assess the applicability of test design techniques is created

[Eld+06]. This method assesses the applicability with the help of eight different points. These points illustrate the different struggles a method can face when it is applied. These points are based on a process of evaluation. Where the model is designed first then second the use case is chosen to apply the model on. Afterwards, the model is applied to this use case. Lastly, it is analyzed and evaluated. This evaluation will provide relevant outcomes for improvements and redesign of the model. The eight assessing points are the following:

1. The faults in the model, where it was hard to apply to the use case
2. The subjectivity of the subject that is assessing the model
3. The ease of applying the model
4. The extent to which the model can be used
5. The generality of the model
6. The number of variants of the model within each scope
7. The possibility to automate the model
8. The overall evaluation of the entire process

These 8 points cover the variation of applicability struggles. Knowing there is a lack of applicability in the current frameworks, this model made itself self-assessing. The self-assessment makes it possible for future models to account for these points. All to make sure that the newly created frameworks have value.

To sum this subsection up, the key challenges for IoT assessment frameworks were identified. How these challenges can be identified is shown by illustrating what the current frameworks lack. Striving for the elimination of these lacks is how IoT-based environments can be assessed. In addition, a risk mitigation model was proposed. To make sure that the impact of cyber risks stays limited.

2.3.3 Risk assessment on the IoT limitations

In the previous subsections, common cybersecurity assessment methods have been discussed. These assessment methods can be used as a baseline to assess new IoT-specific risks. Whenever necessary these methods need to be

elaborated using new types of assessments. In addition, the current limitations of the assessment methods were identified. These limitations need to be overcome using the identified assessment methods. How these are assessed will be discussed in this subsection.

Comprehensiveness overall framework

The comprehensiveness of the overall framework can be measured by the range of assessment methods that are included. In order to be a security assessment method, it is essential to cover all parts of the security environment. Therefore, the frameworks can be assessed on the extensiveness of their assessment methods. Every security framework must cover all relevant assessment components.

Comprehensiveness assessment methods

The comprehensiveness of the assessment methods can be measured by the range of assessments that are included. In order to be a security assessment method, it is essential to cover all parts of the security environment. Therefore, the frameworks can be assessed on the extensiveness of their outcomes. Every assessment framework must cover all parts of the relevant outcomes.

Major challenges for current IoT security frameworks

As identified in the baseline there are five major challenges for current IoT security frameworks [Kar+21]. With the help of their conceptualization and the conceptualization of Nurse et al. [NCD17; Nur+18], it is possible to identify the security risks that need to be assessed.

The first major challenges are the *technical challenges*. Typical challenges here are the challenges of computation power, energy efficiency, cryptography, and architecture. The challenges in making it secure are clear. However, the assessment of the risks, the implemented security standards, the regulatory monitoring, and the maturity suggestions, can help assess these challenges. The risks can be assessed by identifying all the threats, vulnerabilities, consequences, and likelihood of an attack. These can be mitigated by the implementation of security standards. The security standards must solve the 5 NIST values to provide overall guidance. These must be in line with the applicable regulations to ensure the legality of the environment. Finally, the maturity of these security measures must be assessed to create overall

relevant outcomes for the environment. Assessment methods that are especially important for technological challenges are vulnerability assessment methods, network assessment methods, virus detection assessment methods, authentication assessment methods, and penetration testing assessment methods. A last note, in the case that the risks to the environment are too substantial or consist of too much personal (privacy-protected) data, they must meet some minimal requirements to be considered assets.

The second major challenges are the *legal challenges*. These challenges deal with the current regulations and policies on how to deal with cyber violations. Regulations can vary in huge amounts in diverse regions and times. These regulations can focus on security but also in large parts on privacy affecting the legally obligatory security measures. Besides accountability, the policy can have a major impact on the financial and legal consequences for the environment. The special challenge here is that the whole environment must align with the legislation. Therefore, the assessment is simply identifying the current legislation and checking whether all IoT devices can 100% comply with the rules. In addition, legislative monitoring must be in place to properly assess the prosecution and impact of security risks. And to monitor legal developments to anticipate on-time on changes in regulations.

The third major challenges are the *ethical challenges*. These challenges focus on the internal accessibility of the data and the digital ownership of the data. Examples are the integrity of data and information. A key here is access control, where the focus is on the Principle of Least Privilege [VM01]. This principle states that a subject should be given only those privileges needed for it to complete its task. In addition, the subject should only use the privileges to complete that specific task. This makes the challenges operational but also human. To access these challenges it is essential to closely monitor everyone and everything that can retrieve any data. Besides, it is necessary to access the integrity of the subjects that have access to data. The integrity can be measured and assessed with the help of the risk hierarchy framework. Besides, the human assessment method should have a special focus on ethical challenges.

The fourth major challenges are the *operational challenges*. IoT has changed the environments drastically, in terms of the number of devices, diversity of devices, generation of data, and made it a more quickly changing environments. Operationally these environments need to change to handle these changes securely. These operational challenges all fall under the subcate-

gory of management assessment. The management tries to come up with solutions to solve the security issues that come with IoT devices. These have been identified as interconnectivity, things-related services, heterogeneity, dynamic changes, enormous scale, and connectivity. Assessment methods that need to be included to manage these challenges are hardware threats assessment method, policy & countermeasure assessment method, and natural threats assessment method.

The last major challenges are the *adaptive challenges*. These challenges focus on the adaptability of the environments. Identifying future developments and accounts for them in the security assessment. These challenges are covered by the management assessment (organizational adaptivity), regulatory management (regulatory adaptivity), and maturity assessment (advancements). A key assessment method that accounts for these challenges is the human assessment method. The available human knowledge is essential in staying adaptive. Monitoring new trends and research that prove new insights. In addition, strive to stay on top of the maturity to have an advantage when changes are necessary.

Applicability of the framework

The applicability of the framework is often neglected. Testing the applicability can be a complicated task. As proposed before, an eight points framework is designed [Eld+06]. These show how a model can fail in being applicable. However, this also indicates what the exact points are that need to be assessed. These eight points are:

1. The faults in the model, where it was hard to apply to the use case
2. The subjectivity of the subject that is assessing the model
3. The ease of applying the model
4. The extent to which the model can be used
5. The generality of the model
6. The number of variants of the model within each scope
7. The possibility to automate the model
8. The overall evaluation of the entire process

The model, covering these eight points, should be used to test the final created assessment framework. To make sure that the created assessment framework can be applied.

This subsection discussed the methods to assess IoT-based environments. This was structured based on the previously identified limitations of the current assessment methods for IoT-based environments. For all four identified limitations a clear method is proposed. These methods are summarized in the next subsection.

2.3.4 Assessing IoT-based environments

Concluding, this section aims to answer subquestion 2. Formulated as: *"How can risks in IoT-based environments be assessed?"* To answer this question, available and comprehensive assessment methods were introduced. The combination of these assessment methods is used as a baseline to assess the specific IoT challenges. Therefore, the combination of the identified main challenges for IoT assessment frameworks and the comprehensive assessment methods has led to the second intermediate conclusion of this research. This conclusion is also the answer to subquestion 2, and can be summarized as follows:

- **Comprehensiveness overall framework:** The frameworks can be assessed on the extensiveness of their assessment methods.
- **Comprehensiveness assessment outcomes:** The frameworks can be assessed on the extensiveness of their relevant outcomes.
- **Major challenges for current IoT security frameworks:** The five major challenges are technical, legal, ethical, operational, and adaptive challenges.
  - **Technical:** Apply the five components of the comprehensive assessment framework. First, risk assessment that identifies threats, vulnerabilities, consequences, and likelihood of possible attacks. Second, security standards to mitigate these risks. Third, risk management with the help of 5 NIST values. Fourth, legal regulation monitoring. Last, maturity assessment to prepare the environments for future challenges.
  - **Legal:** The assessment is simply the identification of the current legislation and checking whether all IoT devices can 100% comply with the regulations. In addition, legislative monitoring must be

in place to properly assess the prosecution and impact of security risks.

  - **Ethical:** The assessment of ethical values needs to be done by monitoring the Principle of Least Privilege. In addition, the integrity of subjects that have access to the data must be monitored.
  - **Operational:** The assessment of securing the environment must focus on the standardization of devices, the repeating cycle of the assessment, available knowledge within the company, and the suitability of the organizational structure for a secure IoT-based environment.
  - **Adaptive:** The assessment focuses on the internal structure to adapt. Monitoring new trends and research that proves new insights.

- **Applicability of the framework:** The 8 point framework of Eldh et al. can be applied to the final assessment framework [Eld+06].

2.4 Solutions for IoT-based environments

In the previous sections, the limitations of the available cybersecurity assessment frameworks for IoT-based environments were identified. Then, the methods to assess these limitations were discussed. However, a good and comprehensive assessment framework also offers the relevant outcomes to solve the limitations. Therefore, more research is needed to find solutions to these limitations. The question used to discover this is subquestion 3. Subquestion 3 is formulated as follows: *"What are potential solutions to minimize the risks in IoT-based environments?"*

2.4.1 IoT-based environment solutions

The solutions to minimize the risks can be divided into IoT-based environment architecture solutions and current technological trends that work as solutions. In this subsection, the solutions to make the IoT-based environment architecture secure are discussed. Previously, in figure 2.6 the IoT-based environment architecture was shown. Based on these layers, Patel et al. have identified the security requirements at the different layers [PP+16]. In this case, the application and the smart object layers are respectively the sensing and the interface layer. All of these security requirements focus on the technical-, ethical-, and operational challenges of IoT-based environments. This is not comprehensive enough. However, the requirements do form a

strong base for securing the IoT-based environments.

IOT LAYER	SECUREITY REQUIREMENTS
Application	• Application-specific Data Minimization • Privacy Protection and Policy Management •Authentication •Authorization, Assurance •Application specific encryption, cryptography.
Services support	• Protected Data Management and Handling (Search, Aggregation, Correlation, Computation) • Cryptographic Data Storage • Secure Computation, In-network Data Processing, Data aggregation, Cloud Computing
Network layer	• Secure Sensor/Cloud Interaction; • Cross-domain Data Security Handling • Communication & Connectivity Security
Smart object/sensor	• Access Control to Nodes • Lightweight Encryption • Data Format and Structures • Trust Anchors and Attestation

Figure 2.12: *The security requirements at different layer of IoT [PP+16].*

The requirements in figure 2.12 solve the risks that were illustrated in figure 2.7. However, as mentioned before, this does not include all five challenges. Research that did cover the challenges is the paper where the five main challenges are identified. In this research by Karie et al., possible solutions are proposed [Kar+21]. These possible solution are presented in a list of 11 potential solutions that together should solve the five main challenges. These solutions are not all based on existing possibilities but stress what needs to happen in the future to account for secure IoT-based environments. Therefore, not all these points apply to a framework.

1. Develop security assessment frameworks
2. Develop IoT device-specific monitoring tools
3. Implement secure authentications for all IoT devices
4. Encrypt all IoT data

5. Test all IoT hardware before, during, and after deployment
6. Use public key infrastructure security methods in all IoT devices
7. Develop and deploy only secure and trusted IoT applications
8. Implement identity management
9. Generate trust for secure data transmission and object authentication
10. Harden the security of IoT networks, including strong login credentials
11. Regulate and certify IoT devices before the use

In addition, they added that every IoT device is subject to a variety of cyberattacks and that these 11 potential solutions can help to prevent these attacks. However, more solutions can be beneficial. Therefore, they have also added the following six points to the list: IoT security analytics, End-to-end credentials, IoT API security methods, Endpoint detection response (EDR) tools, Dedicated network visibility tools, and Keeping up-to-date with the latest IoT security threats and breaches [Kar+21]. Other countermeasures that were identified by Karie et al. earlier are [KSH20]:

- A multi agent, naive Bayes algorithm, Intrusion Detection System (IDS)
- Machine Learning to automatically classify the attacks
- Multiple point defence mechanism (IoT gateway as IDS)
- Anomaly detector in cloud infrastructure and at the fog computing
- Dynamic update of attack detection model
- Inter and intra-domain collaborative DDoS mitigation
- Mean and standard deviation technique
- Multiple IDS located on the network (edge, fog and cloud IDS)
- IDS function at the edge based IoT-based environment

In combination, solutions were given to the environment on every level. All main challenges are covered. Besides, this last research had a specific focus on intrusion detection whenever the security is vulnerable. Important to these solutions is that the technology is continuously improving [GBB18]. This implies that solutions will always need to be updated to current trends

and technologies. Most of the proposed solutions account for this development by saying that management and methods are needed. For the reason that IoT is a continuously changing environment, we will always need new solutions to the latest threats. In the next subsection, the most recent solutions are discussed.

2.4.2 Latest technological developments in IoT security

The previous subsection illustrated useful methods to secure current environments. However, the best solutions to the main risk will always be the most recent developments in security. For this reason, it is relevant to discuss the latest technological improvements in IoT security. This subsection discusses the most recent trends in encryption, authentication, blockchain, and intrusion detection systems. These values are in line with the most important developments in IoT security mechanisms [Has+19].

Encryption

Encryption is a major challenge for IoT devices. They often have at least one of the following characteristics: small size, limited computational capability, limited memory, or limited power resources. This makes it difficult to use intensive traditional encryption algorithms to secure the information [SSJ20]. Lightweight encryption algorithms offer a solution to these devices. These algorithms focus on providing the best possible encryption with limited computation. The most important primitives are the four shown in figure 2.13. All four play a central role in encrypting and relate to each other in computational needs. Elliptic Curve Cryptography (ECC) is a method to deal with the public key exchange that is illustrated in figure 2.4.

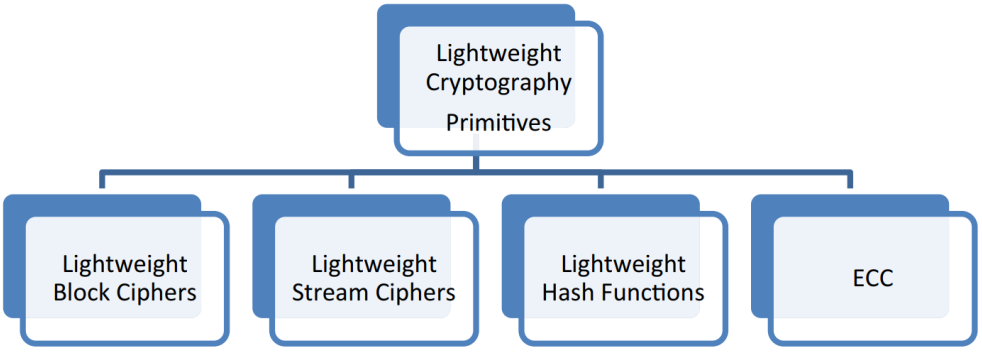

Figure 2.13: *Lightweight cryptographic primitives for IoT [SSJ20].*

The final algorithm and encrypted cipher can be evaluated based on security, chip area, throughput, latency, hardware, and software efficiency, and figure of merit [SSJ20]. Therefore, the best applicable lightweight algorithm is device-dependent. Recent research is done on the current field of lightweight encryption algorithms [SSJ20; TRK21]. They both provide an overview of the performance of the existing available algorithms. In addition, new algorithms keep getting introduced [Gao+21].

Another method used to encrypt data can also be used. This method is called steganography, it encrypts messages in a way that no one suspects that an encrypted message exists [Kha+19]. Steganography is done on top of regular encryption, this means that the data is encrypted first. After this step, a special rule can be introduced to insert this encrypted data into redundant data. This redundant data can for example be an image or other file format. In this way, no one suspects the existence of a secret message. The downside of this encryption is that it increases the size of the data to the size of the data it is hidden in. Also in steganography, there are a lot of different algorithms that can be used [DG21].

Authentication

Currently, the most popular technique to attack network security is still authentication. Just like encryption, proper authentication can be too costly for IoT devices. The most common authentication methods often have too much computational and communication cost [Has+19]. Therefore, authentication methods as mutual authentication, two-factor, multi-factor and biometrics encounter big challenges [LK08; De +13]. This increases the demand for lightweight authentication. However, the environments remain weak to attacks. A selection of these attacks is: stolen verifier, multi-ID, denial-of-service, node capture, replay, forgery, stolen smart-card, sensor-node impersonation, and gateway node bypassing [Has+19].

A survey on the IoT limitations of authentication is done to identify the research necessities [El-+19]. They identified several requirements and open issues that should be taken into consideration by future research and therefore also future authentication assessments. Solutions to solve the most important authentication challenges will therefore mainly focus on the following points:

1. In constrained devices the proposed protocols must be lightweight, making a trade-off between resource consumption and security.

2. The robustness of authentication protocols against potential cyberattacks should be analyzed.

3. The need to consider location and identity privacy in IoT applications.

4. The communication overhead is essential. The number of messages and size of these messages should be kept as low as possible.

5. Low computation costs are essential. The need for lightweight authentication protocols is key in this process.

6. The IoT authentication scheme should be scalable.

7. The authentication service must be aligned to the different layers of the IoT architecture.

8. The heterogeneous devices in IoT-based environments must be considered in the design of an authentication scheme.

9. Hardware solutions can also be used to provide security. Therefore, a combination with software solutions can lead to ideal authentication.

Blockchain

Blockchain is used as a substitute for the important IoT mechanisms trust management and secure routing [Has+19]. Since this technique could solve both problems and is a widely accepted trend to secure data. Blockchain is a relatively new technique that uses a growing list of data structures, called blocks, that are connected and secured by cryptography [BFL20]. The integration of blockchain with IoT could lead to improvements that include the following concepts [Rey+18]:

- **Decentralization** of IoT to become more scalable.
- **Identity regulation**, blockchain can provide trusted authentication.
- **Autonomy of devices**, are capable to interact without servers.
- **Reliability of data**, participants can verify the authenticity of the data.
- **Security of protocols**, can be optimized with the application of blockchain.
- **Market of services**, blockchain can create an IoT ecosystem of services and market places, where transactions are possible without authorities.

- **Secure code deployment**, code can be pushed into devices safely.

The points above are the advantages that blockchain could bring. However, the integration of blockchain also brings challenges along. One of the biggest challenges are the capacity and scalability challenges. Since the storage capacity and scalability of blockchain is still under debate and in the context of IoT applications, the challenge is much greater [Rey+18]. However, there are multiple options to avoid these limitations. The literature proposes multiple techniques to filter, normalize and compress IoT data to reduce the size. In addition, the blockchain method in itself also has vulnerabilities. Limited hashing power can result in a consensus mechanism that is compromised, this would result in a malicious actor that hosts the blockchain. A comparable threat is private keys with limited randomness. In this case, they can be exploited on the blockchain accounts [KS18]. This implicates that blockchain can be a useful method to secure IoT-based environments. However, also brings along its challenges that need to be accounted for.

Intrusion detection systems

Just like many of the challenges, research showed that there is a need to design an integrated IDS that can be applied in IoT-based environments [EAH18]. This means that there is a lack of existing IDSs that are good for IoT. In reaction to this statement new IDSs are introduced. Most of these systems are currently based on neural networks. The first IDS that is introduced is a recurrent neural network (RNN) IDS for IoT [SBW+20]. This IDS has an accuracy score of 95.7%. In the same research, this RNN is optimized to a hybrid convolutional neural network (HCNN). This IDS even provides an accuracy score of 98.6%. Other research that adapts RNN, is a IDS that uses fog computing to create a model [Alm+20]. This model only achieves an accuracy of circa 91% (depending on the training iterations). However, there must be noted that this is another dataset with other characteristics. Compared to other models this is still one of the best models discussed in the research. An understatement is that IDS has an important role in IoT security. The current IDSs with the best quality are all based on neural networks. These neural networks are in some ways adapted to be specifically applicable to IoT situations. However, the main focus must be that the IDS uses the best practice for the specific device. Knowing that IoT-based environments are heterogeneous.

To sum up, this subsection illustrated the most recent technological improvements in IoT security. The trends that are discussed here are encryp-

tion, authentication, blockchain, and intrusion detection. How these technological improvements can lead to more secure IoT-based environments is summarized in the next subsection.

2.4.3 Solutions to minimize risks in IoT-based environments

Concluding, this section wanted to answer subquestion 3. Formulated as: *"What are potential solutions to minimize the risks in IoT-based environments?"* To answer this question, the question was split up into two major subjects.

First, the solutions that relate to the IoT-based environments. Here, solutions for the different IoT architecture layers have been identified together with the main potential solutions for the five main challenges. Additionally, important characteristics of assessment methods were identified. The characteristic is that every assessment is based on the management and method assessment. This is necessary since assessment methods cannot grow at the same pace as technological development.

Second, the most important developments in IoT security mechanisms were discussed. This is done to present the current trends and to include the best solutions to the current threats. The four major trends are encryption, authentication, blockchain, and Intrusion detection systems. The intermediate conclusion that can be drawn after this section, and therefore the answer to subquestion 3, can be summarized as follows:

- **IoT-based environment solutions:** The solutions for a safe IoT-based environment will be a combination of proposed lists. The requirements at different layers from Patel et al. [PP+16]. These can be combined with the 11 future solutions of the baseline [Kar+21]. In this solution, the main focus must be the assessment of good monitoring and management.
- **Latest technological developments in IoT:** The best solutions to the main risk will always be the most recent developments in security. For this reason, it is relevant to discuss the latest technological improvements in IoT security. In IoT security, the most important research topics are encryption, authentication, blockchain, and intrusion detection systems.
  - **Encryption:** Monitor for the latest and best lightweight encryption algorithm that is perfect for the type of device. Whenever possible also add the use of steganography.

- **Authentication:** Solve the main authentication challenges by assessing the nine points of El-Hajj et al. [El-+19].
- **Blockchain:** Solves a lot of security challenges, however, does not apply to every network due to its limitations. Monitor the developments on blockchain to apply whenever the limitations are solved.
- **Intrusion detection systems:** Monitor for the latest and most accurate neural networks that solve the damage that can be done by intruders.

Chapter 3

Methodology

The previous chapter proposed the intermediate conclusions to the first three subquestions. This chapter explains the method that is used to elaborate on and validate these conclusions. In addition, this chapter explains the method used that retrieves information about the last two subquestions. Together, this chapter presents the method that is used to answer the main research question, and therefore the method used to validate the subquestions. This will be done by elaborating on the research strategy first. Afterward, the method for collecting data is discussed. Finally, the method that is used is evaluated. This section elaborates on the methodology discussed in Chapter 1. Here is introduced that this research is *research for design*, that it is based on a qualitative research method, and that it generates a conceptual assessment framework based on the *grounded theory*. This chapter will elaborate on these statements and argue why this method suits this research the best.

3.1 Research strategy

This section elaborates on the method used in this research to answer the research questions. The objective is to research the necessary elements that should be included to assess an IoT-based environment. The IoT elements can be assessed by focusing on their specific characteristics, combined with the methods used to assess the current environments. The outcome of these steps will identify the missing gap in the current assessment methods. Generating the information that needs to be added to these assessment methods to also make IoT-based environments more secure. By identifying this gap, an increase in security in IoT-based environments could be achieved. This gap is identified by answering the following main research question.

RQ: *How to assess challenges and differences in the security of IoT-based environments, compared to the security of traditional computing devices?*

The answer to this question will be an assessment framework. To the best of my knowledge, there does not exist a comprehensive cybersecurity assessment framework for IoT-based environments. Therefore, this research tries to identify and discuss the gap. To achieve this, the method used is based on an exploratory research design. To explore and identify the 'how', in the assessment of these challenges. In addition, the main focus is the design of the assessment framework. Therefore, this research is research for design. This implies that existing research is combined to validate the choices in design.

In addition, the exploratory nature is there to get an insight into the challenges and differences in the security of IoT-based environments. Therefore, knowledge in form of experiences, beliefs, and attitudes is relevant [CP16]. This knowledge can primarily be obtained by interaction with experts in the field. Due to the limited amount of specialists in this field and the maximal amount of information that should be generated by these experts, this research chose to conduct interviews. Interviews are a commonly used method in an exploratory research design with a qualitative research method [CP16].

Qualitative research encompasses the examination of human experience as it appears in people's lives, into facts or principles aimed to describe and clarify these appearances [Pol05]. Qualitative methods can be used as evidence, explaining the causation of the observations. The retrievement of qualitative information by researchers is often done in in-depth interviews [CP16]. To be able to do an in-depth interview, it is necessary to have all the relevant information to the topic. In this case, it was necessary to investigate the research topics of the first three subquestions already. This method was chosen to create the ability to have a more in-depth conversation about the topic and about the most important subjects to discuss. The result is that the interviews will verify the outcomes of these three subquestions. In addition, the interviews encourage the addition of relevant aspects to the answers to the first three questions. Besides, the interviews will explore the overall processes and guidelines that could be implemented and how these could be generalized. The type of interviews will be semi-structured. As the questions in this interview must be substantiated by literature. The semi-structured interviews follow straight guidelines but are also based on intermediate labeling to provide the flexibility to improve the questions or

change direction as new themes emerge and the research progresses. This is beneficial when the same questions asked in the interviews do not retrieve new insights anymore. These interviews will consist of several open-ended questions to gather qualitative data. Further analysis and search for broad patterns in their responses will be done using a method called grounded theory. The implementation of this method is discussed later.

This research is conducted in the Netherlands and is in collaboration with PwC NL. This means that the interviewees are linked to PwC and the research took place within the facilities of PwC. In addition, the research takes place in the first half of 2022.

This section has elaborated on the strategy of the research. It discussed why interviews are used as the main method to retrieve more data. The main reason for this choice was to retrieve as much data as possible from the little number of experts available to the researcher. The next section will elaborate on how the outcomes of these interviews can be transformed into a valid data source.

3.2 Data collection

The previous section has discussed the best method to use to collect valuable data. This section describes the techniques and procedures that are used in the interviews. These methods are relevant to validate the data that is used to answer the main research question and the five subquestions.

3.2.1 The sample and tools

To answer the research questions, it is necessary to verify the identified outcomes of the literature review with experts. In addition, these experts can help explore additional insights. This verification and exploration can be in terms of IoT characteristics and it can be in terms of assessment methods. Therefore, the interviewees can be experts in two different expertises: IoT security experts and cybersecurity assessment experts. In this case, the experts are all part of the network of PwC firms. The employees differ in terms of their expertise, role, experience, education, and country. Roles differ between associate, manager, and director. These roles are fairly aligned with their experience in the field.

As the interviewees work in different countries, it is not possible to do all interviews physically. Therefore, the interviews will be held online. To make the interviews of use, they should be transcribed. The interview can only be transcribed when it is recorded. This means that a meeting tool is needed to connect to the interviewees digitally. This tool must be able to record the meetings. In addition, a transcription function would be desirable in the tool. The tool chosen to achieve this is the Google Meets tool. Google Meets doesn't have a transcription functionality. However, to solve this, Descript is used to do the first transcription of the interviews. The outcomes of this tool were analyzed and corrected.

3.2.2 The interviews

The interviews themselves strive to generate optimal relevant information. This research chose to use semi-structured interviews with open-ended questions. Semi-structured interviews give the process enough flexibility to dive deeper into interesting topics. Besides, open-ended questions generate an open-minded interpretation of the questions. This stimulates out-of-the-box thinking, which is very useful and interesting for both validation and exploration [Jam14]. It enables the interviewee to shape the question to the things they experience to be most important. Furthermore, the interviews will be one-on-one interviews to explore the perspective of the interviewee. This minimizes the chance that the interviewee will change perspective because of groupthink [Jan08]. The questions that are asked in the interviews can be found in Appendix A.

3.2.3 Grounded theory

The outcomes of the interviews must be interpreted as objective as possible. The outcomes must be analyzed and interpreted validly. The most excepted theory used in qualitative research is the grounded theory [SC90]. This method is most excepted because it provides the most guidance to validate the findings. Therefore, this research uses a grounded theory approach. The 8 steps of this process are shown below [Onl09].

1. Identify the substantive area, area of interest
2. Collect data about the substantive area
3. Open code the data when it is collected

4. Write memos throughout the entire process
5. Conduct selective coding and theoretical sampling
6. Sort the memos and find the codes that can organize the codes the best
7. Read the literature and integrate the theory with the codes
8. Write up the theory

Here, open coding and intermediate labeling are two steps in this process that require more explanation. First, open coding is a qualitative approach for identifying the most important concepts discussed in the data. By observing the data and phenomena that are discussed, it is possible to identify important codes. All these codes are attached to the list of codes. This generates a valuable list of codes that are relevant topics that need to be discussed in the remainder of the research. Later these codes will be organized into concepts, subcategories, and categories to create structure and build theory.

Second, intermediate labeling focuses on the determination of the questions in the interviews. This method retrieves the insights and labels of the last interview before the next interview. Using this strategy, the questions of the interview can be changed. It can change the structure, to discuss the topics that were presented to be interesting in the previous interviews. This strategy is based on the work of Strauss & Corbin, they identified the point in development where no new properties or relationships emerge during analysis [SC98]. They created this method to generate the ability to change the interview to keep finding new relevant insights. Therefore, in this research, the transcription and coding of an interview happened between the last interview and the next. An overview of the basic structure of the interviews can be found in Appendix C. Even after intermediate labeling this basic structure is not altered, only the most relevant concepts are more broadly discussed when multiple interviewees considered them crucial.

3.3 Method evaluation

The research method illustrated in the previous sections is proposed to be the best method possible. However, this research method also has its limitations. In the timespan of this research, it was only possible to interview a limited amount of experts. However, the amount of experts available on the relatively new IoT topic is also limited. Therefore, the number of experts

that could be included in this research would always have been low. Using interviews generates the most relevant data per interviewee. Therefore, interviews are the most appropriate method to use in this research. In addition, another limitation is that the variety of experts is low. This is limited because all experts are linked to the same company. Therefore, they may have similar viewpoints and experiences. The positive aspect of doing research within one company is the ease to get in touch with experts around the globe and the relevant expertise that they have. Within PwC a lot of experts are cybersecurity consultants, they will always have an affinity with assessment frameworks.

In addition, interviews are a critique research method due to the subjectivity in the interpretation [CP16]. The grounded theory is the best method to limit this subjectivity in the interpretation. However, the same downside applies to this method. Namely, that the coding is done by a subjective researcher. In this research, this could not be avoided. However, open coding minimizes this subjectivity by forcing the researcher to analyze the data sentence by sentence. Therefore, the chances are high that all important concepts are still identified.

Furthermore, the digital environment of the interviews creates more mental distance between the interviewer and the interviewee than in on-sight interviews [JRT14]. This could decrease the quality of the interaction. Therefore, this must be minimized by encouraging them to put on the camera and have a little small talk previous to the interview.

To summarize, aside from the limitations of the method used, the majority of these limitations could not have been avoided by using a different method due to the scope of this research. The remaining interview-related limitations have been considered in advance, to limit their impact. Together, apart from the limitations of the method, this was the best method available.

Chapter 4

Results

The previous chapter discussed the method used in this research. It elaborated on why interviews are chosen and how these interviews are executed. To follow up, this chapter presents the findings of the data gathered from these interviews. It conceptualizes and analyzes the data to gain additional insights. This will be structured in the following way. The first section presents an overview of the interviews and the interviewees. The second section presents how the interviews have been transformed into structured data. The last section presents the conceptualized findings. Afterward, these findings will be aligned to the subquestions they are related to. Therefore, the last section will discuss the retrieved data structured by every subquestion.

4.1 Overview of the interviews

This section provides an overview of the interviews as well as an overview of the interviewees' experience and expertise. This is presented to validate the outcomes that the interviews generate. First, an overview about the interviewees is presented. In this research a total of ten experts are interviewed. These experts work on a variety of topics that are connected to cybersecurity and/or IoT. These experts work with different clients, depending on the country they work in, the experience they have, and the role they have within that company. In addition, the variation in years of experience results in a variation in the number of clients with whom they have worked. Table 4.1 provides an overview of the roles, years of experience, and countries the experts work in.

Expert	Role	Experience	Education	Country
1	Associate cyberprivacy	1,5 year	Information science	NL
2	Senior associate OT&IoT security	7 years	Technical computer science	DE
3	Associate offensive security	0,5 years	Infrastructure engineering	NL
4	Senior associate EMEA team	2,5 years	Cyber warfare	HU/NL
5	Senior manager cybersecurity	7 years	Business administration	NL
6	Manager data analytics	6 years	Business administration	AE
7	Director OT&IoT cybersecurity	8 years	Electrical engineering	CA
8	Director cybersecurity risk	12 years	Environmental engineering	US
9	Assistant manager cybersecurity	11 years	Electronic communication	IN
10	Pen tester OT&IoT security	2 years	Computer science	DE

Table 4.1: *Overview of the experts.*

Table 4.1 shows that three different roles are included in this research, varying between associates, managers, and directors. The years of professional experience vary between 0,5 years and 12 years (with a median of 6,5 years). Furthermore, the experts are working in 7 different countries, varying over 3 different continents.

Second, the overview of the interviews is discussed. Due to limited traveling possibilities and corona restrictions, all interviews have been conducted virtually. Additionally, these interviews were all in English. This was done to align the outcomes and to make the transcription and coding processes easier. The questions asked in the interviews can be found in Appendix A. The average duration of the interview was: 54 minutes. The interviews ranged in duration between 42 and 72 minutes.

4.2 Codes and categories

The previous section discussed the key characteristics of the interviews and the interviewees. In this section, the results of these interviews are presented. These results were achieved by strictly following the earlier mentioned steps of the grounded theory [SC90]. What data every step provided is illustrated in this section. The first steps that generate data are steps three and four, *open code the data when it is collected* and *write memos throughout the process*. The number of codes that are generated in the interviews after these two steps can be found in table 4.2.

After all the codes are generated, steps five and six of the grounded theory are to *conduct selective coding and theoretical sampling* and *sort the memos and find the codes that can organize the codes the best*. Here, the double and sim-

Interview	Number of codes
1	47
2	58
3	60
4	44
5	70
6	53
7	44
8	77
9	63
10	34

Table 4.2: *Overview of the number of codes per interview.*

ilar codes are joined and translated into concepts. These concepts are structured into categories and subcategories. The full list of these (sub-)categories and concepts can be found in Appendix C. A short version of this list, including the most relevant categories and subcategories, can be found in table 4.3.

Version of May 20, 2022– Created May 20, 2022 - 10:37

Category	Sub-category	Concept
Existing frameworks	Risk framework	CIA
Existing frameworks	Cybersecurity framework	NIST
Existing frameworks	Cybersecurity standards	IEC
IoT	IoT types	IoT/OT/IT
IoT challenges	Technical development	Outdated devices
IoT challenges	IT-OT-IoT convergence	One security framework
IoT challenges	Lack in regulation	Lack in standards
IoT challenges	Size of the environment	Scalability of the attack
IoT challenges	Limited expertise	Human problem
IoT challenges	Interoperability	Reliability
IoT challenges	Adaptability	Not willing to change
IoT challenges	Diversity	Diversity in devices
IoT challenges	Data	Availability
Framework limitations	No existing framework	Outdated frameworks
Framework limitations	No one size fits all	Variety of networks
Framework limitations	Assess static network	Network changes quickly
Framework limitations	Applicability	Generic/specific-trade-off
Framework guidelines	Assessment	Principle based philosophy
Framework challenges	Scope	Holistic network
Framework challenges	Combine frameworks	Not build to fit
Framework challenges	Security by design	Secure before implementation
Framework challenges	Objective assessment	Self assessment
Framework challenges	Flexible framework	Dynamic
Comprehensive framework	Framework testing	Simply cover everything
Comprehensive framework	Framework outcome	Transformation roadmap
Comprehensive framework	Risk assessment	Risk awareness
Comprehensive framework	Management assessment	Conflicting priorities
Comprehensive framework	Maturity assessment	Maturity level
Comprehensive framework	Security standards	All level mitigations
Comprehensive framework	Regulation monitoring	Case specific
Comprehensive framework	Regulation challenges	Responsibility
Comprehensive framework	Environment assessment	Scope of risk
IoT security solutions	Limit attack scalability	Segmentation
IoT security solutions	Limit data traffic	Internal processing
IoT security solutions	Secure architecture	Zero trust architecture
IoT security solutions	Awareness	User training
IoT security solutions	Encryption	Lightweight algorithms
IoT security solutions	Vendor responsibilities	Security by design
IoT security solutions	Secondary security	Boundary defense
Framework guidelines	Framework type	Dynamic framework
Framework guidelines	Existing frameworks	Reusing
Framework guidelines	New framework	Create own vision

Table 4.3: *Overview of the (sub-)categories*

4.3 Mapping data to the research

The previous section concluded with a selection of the generated list of concepts. In this section, this list of concepts is structured per subquestion. This is done by mapping every concept to the question it relates to. Therefore, this section provides a systematic overview of which concepts were relevant to which specific question. Some of the concepts will provide a verifying purpose. These points will emphasize the importance of earlier identified concepts. Additionally, some of the concepts will introduce new insights into the topic. These will generate a broader view of the question, creating a more comprehensive answer to the question.

4.3.1 Subquestion 1

Starting with concepts that were relevant to subquestion one. This question is formulated as follows: *"What are the limitations of the available cybersecurity assessment frameworks for IoT-based environments?"* The most important concepts for this subquestion are illustrated in table 4.4. There is one thing to keep in mind about the tables in this section, they are still a selection of all the concepts found in Appendix C. Only the most important concepts can be discussed, and these tables include only those.

The most important risk and cybersecurity frameworks, that were identified, have already been discussed in this thesis. These frameworks are CIA, NIST, and IEC. Additional relevant risk assessment and cybersecurity frameworks are COSO ERM, ENISA, IoTSF, IRAM2, and ISF. All of these frameworks focus on very specifically defined technology types. Therefore, a clear distinction must be made between IT, OT, and IoT and how these differ. Every type has other characteristics and therefore has to deal with other challenges. The data shows that the challenges related to IoT can still be categorized into the five main challenges (technical, legal, ethical, operational, and adaptive).

The main challenges identified by the data for each of the five main challenges will be discussed here. First, the technical challenges mainly focus on keeping devices up to date with the current security standards. These standards change over time due to new possibilities to secure and attack devices. The main technological challenge is to secure devices with limited capabilities so that they can meet these standards. Second, the legal challenges mainly focus on the limited regulations available to protect and guide en-

SQ1: What are the limitations of the available cybersecurity assessment frameworks?		
Category	**Sub-category**	**Concepts**
Existing frameworks	Risk frameworks	CIA, COSO ERM, and IRAM2
Existing frameworks	Cybersecurity frameworks	NIST, ENISA, and IOTSF
Existing frameworks	Cybersecurity standards	ISO, IEC, and ISF
IoT	IoT types	IT, OT, and IoT
IoT	IoT types	Industrial IoT and consumer IoT
IoT challenges	Technical development	Outdated/not-supported devices
IoT challenges	Technical development	Do not meet security standard
IoT challenges	IT-OT-IoT convergence	Extreme variety in devices
IoT challenges	IT-OT-IoT convergence	Combine into one framework
IoT challenges	Lack in regulation	Conflicting priorities
IoT challenges	Lack in regulation	Bound to contracts
IoT challenges	Size of the environment	Amount of diverse devices
IoT challenges	Size of the environment	Scalability of the attack
IoT challenges	Size of the environment	Attacking surface
IoT challenges	Limited experience	Human problem
IoT challenges	Device related services	Function instead of security
IoT challenges	Operational	Continuous development learn cycle
IoT challenges	Operational	Processes and standards
IoT challenges	Interoperability	Relying on other devices
IoT challenges	Interoperability	Chain of trust
IoT challenges	Adaptability	Limited willingness, priority, and trust
IoT challenges	Connectivity	Always some risk
IoT challenges	Diversity	In devices, software, and networks
IoT challenges	Data	Data protection and availability
IoT challenges	Data	At rest, in transit, and at use
Framework limitations	No existing framework	Immature, incomplete, and outdated
Framework limitations	No one size fits all	Diversity in networks and maturity
Framework limitations	No one size fits all	Combine domain specific frameworks
Framework limitations	Created by industry	Not the highest requirements
Framework limitations	Assess static network	Assessment only captures moment
Framework limitations	Applicability	Generic/specific trade-off
Framework limitations	Applicability	Relevant guidance over all levels

Table 4.4: *Concepts connected to subquestion 1.*

vironments in securing their IoT. Besides, the issue of the vendor/customer contracts is raised, this plays a large part in the possibilities for the customers to secure their IoT-based environments properly. Third, the ethical challenges mainly focus on the conflicting priorities of the vendor, customer, and user. This negatively impacts the chain of trust, while the environment must be built on it. Fourth, the operational challenges mainly focus on managing continuous development without creating security bottlenecks. The implemented processes and standards are key in this and must be managed by someone with expertise. This expertise is needed to deal with a wide range of challenges and to oversee the consequences. Last, the adaptive challenges

mainly focus on the limited willingness of people to continuously develop and improve their security. IoT security is therefore said to be a human problem.

These challenges do not yet concentrate on the issues that an assessment framework has to deal with. The data identified that an IoT cybersecurity assessment framework must converge IT, OT, and IoT to make it operationally useful. Besides, most organizations already use existing frameworks and have a low willingness to change. This has implications for the applicability of the assessment framework. It also has implications for the trade-off that must be made between being a generic or a specific framework. In addition, most assessment frameworks are created by the industry and the industry would never force itself to provide maximal security standards.

To summarize the results of subquestion one, the outcomes of the data are similar to the earlier identified limitations of available cybersecurity assessment frameworks. Where CIA, NIST, and ISO are mentioned as the most important frameworks available. In addition, the five main IoT challenges (technical, legal, ethical, operational, and adaptive) are also identified by the experts. The most important new insights the outcomes provided are the differences between IT, OT, and IoT. Furthermore, some limitations have been identified that all assessment frameworks have to deal with due to the characteristics of an assessment framework.

4.3.2 Subquestion 2

Secondly, subquestion two builds upon the outcomes of subquestion one. After the identification of these limitations, it investigates the possibilities to assess these limitations. This question is therefore formulated as follows: *"How can risks in IoT-based environments be assessed?"* The most important concepts that are identified are illustrated in table 4.5.

The data is divided into three categories. 1) The guidelines for the assessment framework. 2) The challenges that the assessment framework must account for, and 3) The components that the assessment framework needs to have to be a comprehensive assessment framework. The first category identified the guidelines for the assessment framework. This focuses on the sections that an assessment framework should include. It should include an outline, a control section, and an assessment. In addition, it mentions what the philosophy of the framework could be based on. This can either

SQ2: How can risks in IoT-based environments be assessed?		
Category	**Sub-category**	**Concept**
Framework guidelines	Sections	Outline, controls, and assessment
Framework guidelines	Assessment	Rule/principle based philosophy
Framework guidelines	Assessment	Comprehensive and technical dept
Framework challenges	Scope	Holistic
Framework challenges	Scope	IT-OT-IoT convergence
Framework challenges	Combine frameworks	Not build to fit
Framework challenges	Combine frameworks	Familiar with framework
Framework challenges	Security by design	Secure before implementation
Framework challenges	Security by design	Engineer is not a cyberprofessional
Framework challenges	Security by design	Costly erase, so monitor and update
Framework challenges	Objective assessment	Strive to objective self-assessment
Framework challenges	Objective assessment	Descriptive facts
Framework challenges	Flexible framework	Applicable, dynamic, and a loop
Comprehensive framework	Generic/specific trade-off	Generic part applies always
Comprehensive framework	Generic/specific trade-off	Specific parts with help of if-clause
Comprehensive framework	Framework testing	Simply cover everything
Comprehensive framework	Framework testing	Generate all possible threats
Comprehensive framework	Framework testing	Cluster risks semi-automated
Comprehensive framework	Framework outcome	Provide a roadmap with what to do
Comprehensive framework	Framework outcome	Provide guidance and priorities
Comprehensive framework	Framework outcome	Provide (descriptive) feedback
Comprehensive framework	Framework outcome	Illustrate CVE
Comprehensive framework	Framework outcome	Process, validate, and remediate
Comprehensive framework	Framework outcome	3 pillars of transformation
Comprehensive framework	Environment assessment	Scope and scalability of attack
Comprehensive framework	Risk assessment	Risk awareness
Comprehensive framework	Risk assessment	Risk identification
Comprehensive framework	Risk assessment	Product failure
Comprehensive framework	Risk assessment	4 NIST risks
Comprehensive framework	Security standards	Mitigation on all levels
Comprehensive framework	Management assessment	Conflicting priorities
Comprehensive framework	Management assessment	Train user: awareness & best practice
Comprehensive framework	Management assessment	Outdated asset management
Comprehensive framework	Management assessment	Manage access, assets, and people
Comprehensive framework	Management assessment	Manage change and vulnerabilities
Comprehensive framework	Management assessment	Zero day attack
Comprehensive framework	Management assessment	Monitoring: KRI & KPI
Comprehensive framework	Management assessment	Monitor connected to solution
Comprehensive framework	Regulation monitoring	Regulatory stakeholder cycle
Comprehensive framework	Regulation monitoring	Case specific: laws & contracts
Comprehensive framework	Regulation monitoring	Interpretation and compliance
Comprehensive framework	Regulation monitoring	Responsibility
Comprehensive framework	Maturity assessment	Maturity level and security level
Comprehensive framework	Maturity assessment	Corbit and capability framework
Comprehensive framework	Maturity assessment	Organisation maturity
Comprehensive framework	Maturity assessment	Experts and understanding

Table 4.5: *Concepts connected to subquestion 2.*

be rule-based or principle-based. Most experts preferred a principle-based approach. Last, the goal of the assessment framework should be to try to be as comprehensive as possible.

Then the second category identified the challenges for the assessment framework. The scope must be determined to make the assessment framework applicable, useful, and comprehensive. This could be achieved by combining the best existing frameworks. However, these frameworks are not built to fit perfectly, since they have identified other subcategories that do not match one-on-one. In addition, these frameworks focus on assessing what is currently in place. Important here is that a lot of these devices can not be updated easily whenever they are implemented. This means that security by design is a challenge. Since that can not be assessed afterward. Furthermore, an assessment framework is only able to assess a static moment. However, it must be built in a way that makes it more dynamic, to deal with challenges over time.

The third category identified the components of a comprehensive assessment framework. Here we can identify the five subcategories that are identified in figure 2.5. These are risk assessment, security standards, management assessment, regulation monitoring, and maturity assessment. In addition, the environment assessment has been introduced. This is the assessment of the overall scope and the related risks that the environment deals with. In the chain of figure 2.5, this would be placed first in line. As it looks at the highest level of the environment. Furthermore, the data elaborates on the other five subcategories of this model. First, the risk assessment must identify the four NIST risk values (threats, vulnerabilities, consequences, and likelihood) to create awareness. Second, the security standards must mitigate the risks from all security levels, so also the least mature standards available must be included. Third, the management assessment must make the framework more dynamic to create a secure environment to develop and grow security. Specifically focusing on the internal processes and standards that are implemented to monitor and ensure safety. Fourth, regulation monitoring is especially critical in current times due to the fast-changing field and high consequences. Therefore, regulation monitoring is not a subcategory of management. Additional challenges include responsibility, privacy, and interpretation. Last, the maturity assessment is about the final score we can give the environment. Every framework should generate relevant outcomes in some way. Since we want to assess the whole environment it is essential to include the security but also the security maturity of the environment

to rate it with a certain maturity level. This level should be complemented with guidance to improve the level. How this guidance can be provided properly is included in the sub-category framework outcome. Essential in this structure is that everything should be covered. A way to do this is to simply cover everything by using a semi-automated method. This accounts for every possible attack on every point of the environment and does this in a standardized manner.

To summarize the results of subquestion two, these outcomes have focused on three categories. 1) The guidelines for the assessment framework. This issued the importance of a principle-based philosophy and an outline, control, and assessment section. 2) The challenges that the assessment framework must account for, dealing with issues that are hard to solve by assessment frameworks. And 3) the components that the assessment framework needs to be a comprehensive assessment framework. Adding the environment assessment to the list of most important components.

4.3.3 Subquestion 3

Thirdly, subquestion three counters these risks that we need to be assessed. After identifying how these risks can be assessed, it tries to find solutions for these risks. This question is therefore formulated as follows: *"What are potential solutions to minimize the risks in IoT-based environments?"* The most important concepts that are identified are illustrated in table 4.6.

These concepts differ in how they offer security. The first group of solutions strives for maximal security in the architecture. These concepts are standardization, segmentation, internal processing, zero trust architecture, end-to-end encryption, the principle of least privileged, and the safe fail system. These concepts would theoretically solve the most important IoT cybersecurity challenges. However, the complete implementation of these solutions is hardly possible. Therefore, to counter specific attacks, additional measures such as the enforcement of minimal controls and user training must be implemented. These measures provide security but are only useful whenever minimal security controls are implemented. One of the most important solutions for all IoT-based environments would be stronger regulations. Regulations enforce every part of the chain to do its part in securing the environment. This cannot be implemented by an environment but is crucial in the road to secure environments. In addition to the standard solutions, security software exists that identifies security threats and helps in securing

SQ3: What are potential solutions to minimize the risks in IoT-based environments?		
Category	**Sub-category**	**Concept**
IoT security solutions	Limited protocols	Standardization
IoT security solutions	Limited protocols	Enforce minimal controls
IoT security solutions	Limit attack scalability	Segmentation
IoT security solutions	Secure data traffic	5G bandwidth: encryption
IoT security solutions	Limit data traffic	Internal processing
IoT security solutions	Limit data traffic	Data mitigation
IoT security solutions	Secure architecture	Zero trust architecture
IoT security solutions	Secure architecture	Basic cyber hygiene
IoT security solutions	Secure architecture	Product life cycle
IoT security solutions	Secure authentication	lightweight algorithms
IoT security solutions	Awareness	User training
IoT security solutions	Encryption	lightweight algorithms
IoT security solutions	Encryption	End-to-end
IoT security solutions	Critical	Analog
IoT security solutions	Privacy	POLP
IoT security solutions	Vendor responsibility	Vendor regulation
IoT security solutions	Vendor responsibility	Security by design
IoT security solutions	Security enforcement	Regulations
IoT security solutions	Secondary solutions	Firewall
IoT security solutions	Secondary solutions	Patching
IoT security solutions	Secondary solutions	Access control list
IoT security solutions	Secondary solutions	Threat landscapes
IoT security solutions	Secondary solutions	Boundary defense
IoT security solutions	Secondary solutions	Safe fail system
IoT security solutions	Security software	Azure, Nozomi, Dragos, and RMIS

Table 4.6: *Concepts connected to subquestion 3.*

the environment. Currently, some of the most valuable software available are Azure, Nozomi, Dragos, and RMIS.

To summarize the results of subquestion three, there are a lot of different possibilities that could improve security. Some are more theoretical and some are more operational. The most important thing is that different types of threats need different types of solutions. Therefore, the implemented solutions should fit the threats in the environment. Security software can be very useful in identifying threats. However, strong regulations are the most important solution to achieve secure environments.

4.3.4 Subquestion 4

Fourthly, the earlier identified outcomes of the limitations, assessment methods, and solutions need to be combined into processes or guidelines to improve security. Therefore, this question is formulated as follows: *"What overall process or guidelines can be implemented to improve the security of IoT-based environments?"* The most important concepts that are identified are illustrated in table 4.7.

SQ4: What overall process or guidelines can be implemented to improve the security of data in IoT-based environments?		
Category	**Sub-category**	**Concept**
Framework guidelines	Scope	Distinguish public/private network
Framework guidelines	Scope	Distinguish IT/OT/IoT
Framework guidelines	Scope	Distinguish industrial/mainstream IoT
Framework guidelines	Framework type	Dynamic
Framework guidelines	Framework type	Build on best practice
Framework guidelines	Existing framework	Already in use and understood
Framework guidelines	Existing framework	Value existing framework
Framework guidelines	Existing framework	Reuse the included knowledge
Framework guidelines	Create value	Make it worth to use new

Table 4.7: *Concepts connected to subquestion 4.*

These concepts offer important guidelines to follow when a new assessment framework is developed. The first important thing here is the scope of the assessment framework, which must be very well defined to distinguish it from certain special cases. In addition, to deal with the fast-changing environments. The assessment framework should strive to be dynamic. How to achieve this should be substantiated by the best practice. The best practices available are the currently most used assessment frameworks. These have implemented a method to deal with this issue. Furthermore, in cybersecurity, it is hard to be comprehensive when you base the framework on a limited number of researches. In addition, the currently best frameworks are very useful and are based on much more research and expertise. These frameworks also show the best types for a framework that are available. However, in the process of creating the assessment framework, it is essential to create value. A new assessment framework must add enough new insides to distinguish it from previous assessment frameworks. This means that the created assessment framework must add enough value to convince IoT-based environments to switch their practice.

To summarize the results of subquestion four, the processes and guidelines that can be implemented should be inspired by the best practices available. Currently, the best practices are the most used frameworks. Here a clear focus must be on the scope that is included in the process or guidelines. Based on this scope, the guidelines and processes must create value to retrieve relevance in improving the security of IoT-based environments.

4.3.5 Subquestion 5

Lastly, the outcomes of the previous subquestion provided guidance for new processes and guidelines. Compared to the previous question, this question explores what specifics can be implemented and what this implementation should be based upon to make the assessment framework valid. This question is formulated as follows: *"How can the IoT-based environment security be generalized into an overall applicable assessment framework?"* The most important concepts that are identified are illustrated in table 4.8.

SQ5: How can the IoT-based environment security be generalized into an overall applicable assessment framework?		
Category	**Sub-category**	**Concept**
Framework guidelines	Reusing in security	All based on experience and knowledge
Framework guidelines	Reusing in security	Base on existing research
Framework guidelines	Reusing in security	Base on existing frameworks
Framework guidelines	New value	Be innovative
Framework guidelines	New value	Create own vision
Framework guidelines	Validate	Use the four eyes principle
Framework guidelines	Validate	Check with experts

Table 4.8: *Concepts connected to subquestion 5.*

Important here is that the new assessment framework must be based on existing work. This can either be an existing framework or research. Both are based on valid grounds. In addition, value can be created by innovative ideas. These ideas can be based on personal vision but should be substantiated by comparable research. Furthermore, the final assessment framework that is created, should also be validated. This can be done by critical experts that evaluate the assessment framework. This step is essential, due to the importance of the four-eyes principle in cybersecurity. To make sure that no obvious mistakes are made or important aspects are forgotten.

To summarize the results, the security of IoT-based environments can be generalized into an overall applicable assessment framework. The structure

of how this research provided solid ground for this assessment framework is visualized in figure 4.1. As shown in the figure, this assessment framework is the final answer to the main research question. It is based on the best research and the best frameworks available. Together, these include the most valuable and valid knowledge. The value that the new assessment framework will create can be increased by being innovative and by validating the result.

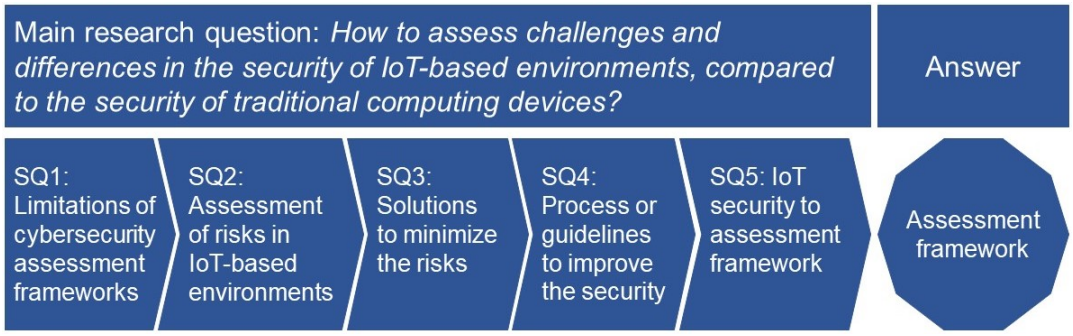

Figure 4.1: *Overview of how this research is structured.*

Version of May 20, 2022– Created May 20, 2022 - 10:37

Chapter 5

Discussion & design

This chapter discusses the outcomes of the collected data that are discussed in the previous section. It fulfills step seven of the grounded theory, to *read the literature and integrate the theory with the codes*. Therefore, the data is combined with the earlier discussed literature. Whenever relevant new insights come to light, these will be substantiated by research. This chapter evaluates the overall data and its implications for the final assessment framework. In addition, the choices that are made in the design of the assessment framework are explained here.

5.1 Limitations of security assessment frameworks

In an earlier stage, four different categories of limitations have been identified. Firstly, the comprehensiveness of the framework. Secondly, the comprehensiveness of the outcomes that are provided by the framework. Thirdly, the five main challenges for IoT-based environments (technical, legal, ethical, operational, and adaptive). Lastly, the applicability of the framework. The later retrieved data provided the following additional insights.

In the data, the limitations of the security assessment frameworks can be divided into two groups. The first group focuses on the current frameworks. This first group identifies the limitations of these frameworks. In addition, the main struggles to create a framework are identified. The current frameworks are often not comprehensive and the relevant outcome of these frameworks is limited. In addition, they are immature, incomplete, and outdated. Besides, they often fail to give relevant outcomes on all different security levels. Since most frameworks focus on environments with very high security

standards. As stated earlier, the most important frameworks are CIA, NIST, and IEC. All these frameworks are already included in the baseline of Karie et al. [Kar+21]. However, contrary to what was stated in the baseline there do exist some IoT-specific frameworks. These frameworks focus specifically on IoT and offer a baseline, guidelines, or good practices for environments and devices. In combination, these frameworks generate enough value to function as a starting point for a new framework. The most relevant identified frameworks are ENISA publications, IoTSF, and IEC 62443 [Lel21; WG121; Com18]. These three frameworks have identified IoT solutions. To come to these solutions they have identified IoT overall. Combining these definitions a new definition will be proposed that encompasses all the included devices. In this way, the different IoT types that are included are identified. The need for identifying these types is a result of the diversity in IoT devices. Determining the exact scope creates a more specific target to assess. This helps in making the assessment framework more applicable. In addition, to make the assessment framework useful and applicable to environments, it is necessary that the assessment framework convergences between IT, OT, and IoT devices. Therefore, the new assessment framework will not differ much from the current standards. This is done to make the transition easier, this is desirable since it will attract more environments. A broader reach will increase the willingness to improve the assessment framework. Besides, the use of the current standards makes the assessment framework more comprehensive and gives guidance in ways to provide useful outcomes.

The second group of limitations derived from data focuses on the most important challenges for IoT devices and their environments. Verifying the challenges that were identified earlier, all the newly identified IoT challenges can be placed under five categories. These are technical-, legal-, ethical-, operational-, and adaptive challenges. However, the specifically identified concepts that are related to these challenges differ from the baseline. This only means that the included subcategories of these challenges are even more extensive than predicted earlier. Therefore, the challenges become even more important to solve. This implies that the challenges must get a central role in the final framework. In combination, both groups verify the four earlier identified categories. Nevertheless, the data was able to broaden the view of the relevant limitations and solutions to these limitations.

In conclusion, these two groups will affect the assessment framework as follows. The assessment framework should be based on NIST, CIA, and IEC since these have shown to have a lot of value. In addition, the work

of ENISA, IoTSF, and IEC 62443 should be added to these works. This implies that the scope must include the scopes that these three frameworks cover collectively. Furthermore, within this assessment framework, the difference between the five main challenges should be highlighted to generate structure.

5.2 Risks assessment in IoT-based environments

The previous section showed that risks can be assessed with the help of an applicable and comprehensive assessment framework. To find the right format and method to assess these risks, it is essential to know how these risks can be assessed. Earlier, the categories that need to be assessed have been identified. These include the comprehensiveness of the framework, the comprehensiveness of the outcomes, the way to assess the five main challenges, and the applicability of the framework. The later retrieved data provided the following additional insights.

The data is categorized into three different categories. The first category focuses on the framework guidelines. These guidelines show that a framework needs at least three different sections. These sections are the outline, the controls, and the assessment. Only when these three are included, an assessment framework can become applicable. In addition, the assessment can differ in a variety of philosophies and designs. In every case, the new assessment framework must include these three sections.

The second category focuses on the framework challenges. These include the possible pitfalls and identify the issues that every framework needs to overcome. First, the determination of the scope is complex since there are almost always special cases to which some challenges and solutions don't apply. The previous section states that the scope of the framework will be covering the widest scope that can be included. Second, the combination of frameworks, which would in many cases be ideal, is hard since they are not designed to fit together. However, the relevant information the frameworks include should be included in the best way possible. Third, security by design is a major issue in cybersecurity frameworks. Whenever a device is operating it is extremely costly to replace these devices. In addition, engineers are not security professionals which makes it hard to secure every device at a later point in the development cycle. This can be solved by security by design and risk assessment that shows that it is beneficial to secure the device. Fourth, objective assessments are hard to achieve. Questions that

can be interpreted subjectively could influence the outcome negatively. This could be attacked by striving for descriptive facts and clear boundaries in the assessment. Last, the framework should be dynamic. Usually, a framework can only assess a static point in time. However, a framework should be able to perform relevant estimations of how the environment will perform in the future. This implies that the framework should have dynamic capabilities (e.g. KPIs, KRIs) to maintain security.

The third category focuses on a comprehensive framework. It identifies the essential parts that need to be included in a comprehensive assessment framework. In figure 2.5 many of these elements have already been identified. However, also the environmental assessment showed to be of crucial value. Therefore, the new fishbone diagram can be found in figure 5.1. Every category has its consequences for the framework. The final framework will address each of these categories.

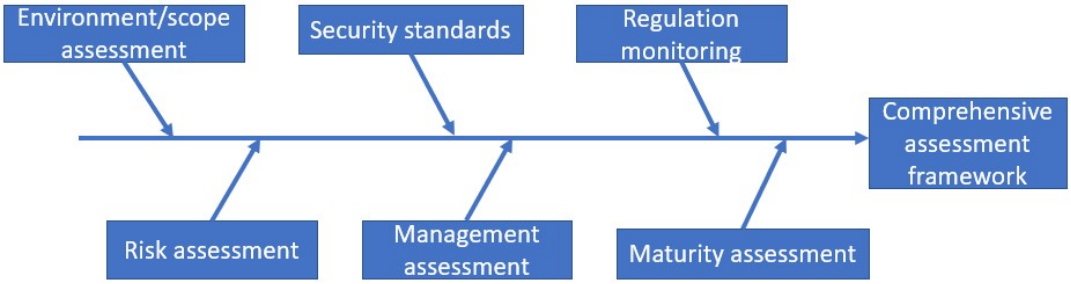

Figure 5.1: *Fishbone diagram of the architecture of an comprehensive assessment framework.*

In addition, the most relevant outcomes of the framework have been identified. They should provide a roadmap that identifies what to do and in what order. In this roadmap, it is important to provide guidance and prioritize the issues. To keep this objective, a lot should be based on descriptive feedback of facts. In addition, the roadmap should be based on the people, process, and technology (PPT) model of transformation [Sch01]. This implies that the framework's outcome will provide priority in what order and how to improve the environment.

In conclusion, the importance of the comprehensiveness of the assessment framework, the comprehensiveness of the outcomes, the way to assess the five main challenges, and the applicability of the assessment framework is verified. These first two categories and the last category should be

considered in the evaluation of the assessment framework. The five main challenges (technical, legal, ethical, operational, and adaptive) should be included in the assessment framework to generate structure. These four categories should be covered by the 6 assessment elements, illustrated in figure 5.1, that should be included in the assessment framework.

5.3 Solutions to risks in IoT-based environments

The previous section showed how the risk could be assessed. In addition, a comprehensive assessment framework should provide a roadmap to improve the security of the environment. To be able to provide a roadmap, possible solutions must be identified. In an earlier stage, possible solutions were divided into two groups. The IoT-based environment solutions and the latest technical developments. The later retrieved data provided the following additional insights.

The provided solutions vary a lot in what they solve and how they relate to the environment. Due to the elaborateness and diversity of the solutions, these will not be discussed individually. However, the main concepts that are identified will be aligned with the previously retrieved solutions. Because these concepts do not fit one-to-one they are aligned focusing on the same problem. Some of these concepts do not fit together. These will be illustrated individually.

As shown in table 5.1, most of the solutions that were retrieved from the literature can be verified by the interviewees. In addition, some new insights have been gained. Vendor regulation is identified as a solution to legal challenges. These regulations would have an important impact on the *chain of trust* and *security by design* concepts. The importance of these regulations can be substantiated by the work of Lata and Kumar [LK21]. They have identified the importance of regulations in IoT security. Furthermore, a safe fail system should be included that makes sure that whenever the system fails it does something secure (e.g. a drone that stays in the same place whenever it is out of reach). The importance of such a mode can be substantiated by Qiu et al. [Qiu+21]. They have tested a fail-safe mode in a critical system.

In conclusion, the range of solutions to improve the security of IoT-based environments is very broad. Here, most solutions that were retrieved from the literature can be verified by the interviewees. In addition, the solutions retrieved by the interviews can be backed by newly introduced research.

From literature retrieved solutions	From data retrieved solutions
Data minimization	Data mitigation
Privacy protection & policy management	POLP
Authentication & identity management	Lightweight algorithms
Cryptography on all levels	End-to-end and lightweight algorithms
Protected data management and handling	Basic cyber hygiene and internal processing
Secure computation	Basic cyber hygiene
Cross domain data processing	Segmentation and standardization
Secure sensor interaction	Basic cyber hygiene and 5G bandwidth
Access control	Access control list
Data format and structure	Enforce minimal controls
Trusted anchors and attestation	Zero trust architecture and analog
Device monitoring	Product life cycle
Hardware testing (before/during/after)	Security by design and product life cycle
Only deploy secure device	Security by design
End-to-end credentials	End-to-end
Endpoint detection response (EDR)	Threat landscapes and boundary defense
Keeping up-to-date	Patching
Intrusion detection system (IDS)	Threat landscapes
User awareness	User training
Security software	Firewall and security software
Domain collaborative DDoS mitigation	
Blockchain	
Authorization (assurance)	
Security analytics	
API security	
	Vendor regulation
	Safe fail system

Table 5.1: *Align earlier and new solutions.*

Therefore, all the identified solutions will be included in the assessment framework as solutions to improve the security of the IoT-based environments.

5.4 Securing data in IoT-based environments

The previous section showed how some of the risks could be solved. The solutions have a high variety of problems they individually solve. Therefore, the following question remains: *What overall process or guidelines can be implemented to improve the security of IoT-based environments?* The retrieved data that answers parts of the question is provided here.

The first guideline is to determine a clear scope. This will be done by cre-

ating a clear definition of IoT-based environments. As discussed before, this definition will be a combination of the definitions of the existing frameworks that are included. Within this scope, it is essential to identify the coverage of IT, OT, and IoT. As proposed in section 5.1, ENISA, IoTSF, and IEC will be used as a baseline in this framework. Therefore, we look at their definitions. First, ENISA has defined IoT as "a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making" [Lel21]. Second, IEC has defined it as "a global network used to interconnect embedded objects such as sensors and mobile devices" [Com18]. Third, IoTSF includes the business processes, the "Things" in IoT, i.e. network connected products and/or devices, aggregation points such as gateways and hubs that form part of the connectivity, and networking including wired, and radio connections, cloud and server elements. As IoTSF is already focusing on the IoT-based environment, the combination of ENISA and IEC suits better. Therefore, IoT will be defined in the assessment framework as: "A global cyber-physical network of interconnected embedded objects". Including all IT, OT, and IoT devices that are somehow connected to the internet.

The second guideline is to make the assessment framework dynamic. This can be achieved by following the best practice available. Currently, one of the best and most practiced frameworks is the NIST cybersecurity framework [Ali+20]. This framework identifies five phases of security and includes its management. In addition, it is presented as a repetitive cycle. For these reasons, it accounts for the continuous development and monitoring of the security of the environment.

In addition, using NIST is in line with the third guideline. This guides the assessment framework to be based upon existing frameworks. This is a good practice since existing frameworks are already understood and used in practice. This makes the transition for environments less costly. Furthermore, the best framework available is most likely to be validated and based upon the most important and valuable knowledge in the field. NIST is considered a comprehensive assessment framework, it included the categories illustrated in figure 5.2.

The last guideline focuses on the creation of value. It should be worth the effort to create a new assessment framework. This implies that enough value should be added to the existing NIST framework. This is necessary to make environments consider switching from the framework they are using to the newly created assessment framework.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 5.2: *Function and Category Unique Identifiers of the NIST cybersecurity framework [SN12]*

In addition to the retrieved data, there also exists research on this topic. Firstly, an overview is given on the existing IoT assessment methods that are relevant to IoT-based environments [AH19]. A list of these methods is given in table 5.2. In this table, these methods are aligned to either technical- or physical security.

This distribution of assessment methods could be a structure to counter the IoT-specific challenges. However, in this research, the alignment to NIST

Technical security	Physical security
Vulnerability assessment method	Human assessment method
Network assessment method	Hardware threats assessment method
Virus detection assessment method	Policy & countermeasure assessment method
Authentication assessment method	Natural threats assessment method
Penetration testing assessment method	

Table 5.2: *List of assessment methods for IoT assessments [AH19].*

is chosen to limit the transition complexity. These 9 assessment methods will be part of the assessment framework. Secondly, a list of points to focus on in IoT software assessment frameworks is given [Lia+21]. A lot of these points are already included in previous sections. Therefore, only the newly introduced points will be presented in table 5.3. The included additional points must be included in the assessment framework as guidelines to focus on in IoT-based environments.

Maximum signal range	Quality of wireless communication technology
Throughput and data rate	Secure auditing
Trust	Reputation
Accountability	Resilience to attacks
Fault tolerance	Culture
Heterogeneous network recognition	Node information certificate
Secure cloud computing	Application security

Table 5.3: *List of additional points to focus on in IoT software assessment framework [Lia+21].*

To conclude this section, the NIST cybersecurity framework will be used as a baseline. This will be complemented with the most important IoT frameworks. These frameworks are ENISA, IoTSF, and IEC 62443. In addition, more solutions from research and retrieved data will be included to get a maximum range of information into the assessment framework. In this creation, the 6 elements of figure 5.1 must be seen as overall guidelines of the assessment framework.

5.5 IoT-based environment security framework

The previous section described what the baseline of the new assessment framework is. In this section, the choices made to fit all the information from research and interviews together will be discussed. In addition, the concepts retrieved from the interviews will be included in the framework. So

the valuable available information is used maximally. In addition, the new assessment framework should add enough value to the existing frameworks that the result positively differentiates from existing frameworks. The final generalization of the assessment framework must be validated by experts to retrieve even more value. The frameworks and data points that are included in the final assessment framework will be discussed individually.

5.5.1 ENISA

Starting with ENISA, ENISA is the European Union agency for cybersecurity. This agency has done a lot of research on IoT and how to secure it. In this research, three different ENISA publications are included. First is ENISA's good practices for IoT and smart infrastructures tool [Gin+17]. Second is good practices for security of IoT - secure software development lifecycle [Sko19]. Last is guidelines for securing the IoT - Secure supply chain for IoT [Sko+20]. How the information stated in these publications is included in the framework is described below.

Starting with the baseline 'good practices for IoT and smart infrastructure tool' [Gin+17]. This tool describes IoT-specific security measures and good practices. These are all placed in a specific security domain. The security domains in the tool can be found in table 5.4. This table illustrates how these measures relate to the NIST unique category identifiers. This thesis does not propose these security domains and unique category identifiers to fit one-on-one but proposes the best fit possible. In addition, the measures in the ENISA tool are mapped to a category. The ENISA categories include technical measures, these will be included in the technical challenges. They include policies, these will be included in the legal and ethical challenges. Lastly, they include the section organizational, people, and process. These will be included in the operational and adaptive challenges. Also, these ENISA categories are not designed to fit one-on-one to the identified challenges. However, to be comprehensive, they must be included in all categories to which they may be relevant.

Secondly, 'good practices for security of IoT - secure software development lifecycle' are identified [Sko19]. These good practices are split into three different categories. People, processes, and technologies. Here, the category people are always mapped into PR.AT, the challenges it will link to will be subcategory specific. The category processes will always be linked to

ENISA security domain	Related NIST UCI
IT Security Architecture	ID.AM & PR.DS, IP
Information System Security Goverance	ID.GV & PR.AT
Risk Management	ID.RA, RM
Identify and Access Management	PR.AC
Ecosystem Management	PR.PT
IT Security Maintenance	PR.MA
Computer Security Incident Management	DT.AE & RS
Physical and Environmental Security	PR.AC & DT.CM
IT Security Administration	ID.GV
Continuity of Operations	PR.MA & DT.CM & RC
Detection	DT
Crisis Management	RS & RC

Table 5.4: *ENISA domain linked to NIST unique category identifiers.*

the operational challenges. Here, the category it is linked to is subcategory specific. The category technologies will always be linked to the technical challenges and the category it is linked to is subcategory specific.

Finally, 'guidelines for securing the IoT - Secure supply chain for IoT' are proposed [Sko+20]. As the title indicates, this article highlights the issues in the supply chain. Therefore, the guidelines raised in the research are mapped into ID.SC. The challenges they are mapped to depend on the final guideline they are related to. In addition, the solutions are added to the other categories that have similar guidelines.

5.5.2 IoTSF

In addition, the IoT Security Foundation (IoTSF) has created an IoT Security Assurance Framework. This framework is discussed here, it has identified fourteen different assurance topics. These topics focus on where IoT-based environments should focus on to make their environment more secure. Therefore, these topics are valuable to map to the baseline. IoTSF included what part of the organization is responsible for these topics. These topics are mapped to the NIST categories based on the description of IoTSF. IoTSF described who is responsible for every topic using keywords. These can therefore be mapped using the main IoT challenges. How these IoTSF keywords are mapped to the main IoT challenges can be found in table 5.5. Together, the topics are mapped to the right place in the baseline.

First keyword IoTSF	Second keywords IoTSF	Main IoT challenge
System	Software	Technical
System	Hardware	Technical
System	Physical	Technical
Business	Process	Operational
Business	Policy	Legal
Business	Responsibility	Ethical

Table 5.5: *How IoTSF keywords are mapped to main IoT challenges.*

5.5.3 IEC

Moreover, the IEC 62443 standards are a special case compared to the two previously discussed cases [IEC20]. As IEC is already included in the baseline research of Karie et al. [Kar+21] and it is also already included in the current NIST framework. However, IEC 62443 consists of multiple sections, and not all of these are included. IoT devices are especially reliant on security by design, due to the limited possibilities to patch devices. The IEC 62443-4 sections are not included in NIST but are essential in providing feedback to these components. It helps IoT device manufacturers in their product development lifecycle and helps to produce secure IoT products. Therefore, the NIST framework should be added with the IEC 62443-4 sections [LČH19]. The 62443-4 section includes two subsections. The first subsection is IEC 62443-4-1, this section discusses the product development requirements. These standards are mapped to the operational challenges. The second relevant section is IEC 62443-4-2, this section discusses the technical security requirements of the system. These standards are mapped to the technical challenges.

5.5.4 In research found solutions

Finally, besides the existing frameworks, this research has summed up numerous good practices for IoT-based environments. All these researches add value as they emphasize the importance of the topic they discuss. Therefore, this subsection will explain how these researches are included in the framework.

The first research that is included, is an overview of the relevant IoT assessment methods [AH19]. These assessment methods were organized in the physical-, information-, and social domain. Here, the assessment methods in the physical domain are mapped to operational challenges, the assessment methods in the information domain are mapped to technical challenges, and the assessment methods in the social domain are mapped to ethical challenges. How these methods are mapped to categories in the assessment framework can be found in table 5.6.

Assessment method	**NIST UCI**
Hardware threats	ID.AM & PR.DS
Policy & countermeasure	ID.GV & PR.IP, PT
Natural threats	ID.RA
Vulnerability	ID.RA & PR.IP & DT.CM
Network	PR.AC, PT & DT.AE, DP
Virus detection	DT.AE, CM, DP
Authentication	PR.AC
Penetration testing	ID.RM & DT.CM, DP
Human	PR.AT, IP

Table 5.6: *Assessment methods of Aboelfotoh and Hikal (2019) mapped to NIST unique category identifiers.*

The remainder of the important topics that are included in this research, are illustrated in table 5.1. For every alignment, one concept will be identified. In addition, this will be mapped to a NIST category and one of the main challenges. An overview of this mapping is given in table 5.7.

Solution concept	Main challenge and NIST UCI
Data mitigation	Operation: ID.RM & PR.IP
Privacy protection	Legal & Ethical: PR.DS, IP
Authentication	Tech: PR.AC
Cryptography	Tech: ID.AM & PR.DS, IP
Basic cyber hygiene	Operation: ID.GV, RM & PR.MA
Internal processing	Tech: ID.AM
Segmentation & standardization	Tech & Operation: ID.AM, RA, RM & PR.AC
Secure sensor interaction	Tech: PR.PT & DT.DP
Access control	Tech & Operation: PR.AC
Enforce minimal controls	Tech & Operation: ID. AM, GV, RM, SC & PR.MA
Trusted anchors & attestation	Operation: ID.RM & PR.IP
Device monitoring	Operation: DT.CM
Hardware testing	Operation: ID.AM, SC & PR.DS, MA
Security by design	Legal & Ethical: ID & PR & DT.CM
End-to-end credentials	Legal: PR.AC
Threat landscapes & boundary defense	Tech: ID.RA & PR.PT
Patching	Operation: ID.GV & PR.MA
Intrusion detection system (IDS)	Tech: DT.CM, DP
User awareness	Operation: PR.AT
Security software	Operation: DT.DP
DDoS mitigation	Tech: ID.RA & RS.MI
Blockchain	Tech: PR.PT
Authorization	Tech: ID.AM & PR.AC, DS, IP
Security analytics	Operation: ID.AM, GV & DT.CM
API security	Tech: PR.DS, IP, PT
Vendor regulation	Legal: ID.AM, GV, SC & PR.MA & RC.CO
Safe fail system	Tech: ID.AM, RA & PR.PT & RS.RP

Table 5.7: *Identified solutions mapped to the framework.*

In conclusion, this section discussed how the related frameworks and researches are generalized into an assessment framework. This framework was able to include most of the important characteristics of an IoT assessment framework. However, the applicability of the assessment framework is not yet tested and the assessment framework as a whole is not yet validated by experts. In addition, the responsibility for the most important regulatory challenges lay with regulators. As regulators are the only ones that can enforce security on different levels. As a result, these challenges cannot be solved by a assessment framework. However, guidelines for what regulators need to focus on in enforcing security can be found in the assessment framework. These limitations imply that the final assessment framework is not flawless yet. However, it does provide a lot of guidance for best practices in IoT-based environments. In addition, IoT security is still a fast-changing field that must be monitored and updated over time. There is no exception to this assessment framework.

Chapter 6

Assessment framework

The previous chapter substantiates the choices made in the assessment framework. This chapter provides the cybersecurity assessment framework for IoT-based environments. It presents the answer to the main research question of this thesis. The reason to choose this format is explained here, as well as how to interpret the assessment framework. In the end, the outcome of this research is presented and evaluated.

6.1 General outline

This assessment framework is created to guide builders of IoT-based environments to improve their security. In this assessment framework, IoT is defined as a global cyber-physical network of interconnected embedded objects. Where IoT-based environments also include business processes, aggregation points (form part of the connectivity), and networks (the possibilities for connection). The goal is therefore to improve the security of the embedded objects, business processes, aggregation points, and networks.

As identified earlier, this assessment framework must converge between IT, OT, and IoT to be comprehensive and generally applicable. NIST is currently the most applied IT framework and also includes the most important OT guidance [Bar+18]. This is the main reason why the NIST cybersecurity framework is used as a baseline. To become comprehensive and include IoT in this assessment framework, IoT guidance will be added to the current assessment framework. This implies that whenever an IoT-based environment is being assessed, it should first follow the existing guidelines of NIST. When that is done, this assessment framework can be applied to assess the security

of the IoT-based environment.

Other benefits of choosing the NIST framework as a baseline are that it provides the ability to self-assess. Besides, the NIST framework introduces the four important parts of risk assessments (threat, vulnerability, consequence, and likelihood), which this assessment framework will be elaborating on. In addition, it provides context on how to manage risks. Furthermore, the NIST framework provides the possibility to prioritize different categories with different security standards. Altogether, NIST includes the most essential parts necessary in an assessment framework.

6.2 Controls

This section will explain how the cybersecurity assessment framework for IoT-based environments should be interpreted. This will be done by focusing on the following different parts of the framework. The environment assessment, the additions to the NIST framework, the outcome, and how these lead to guidance for the IoT-based environment.

Firstly, the environment assessment. Here, the first three steps of the NIST subsection *Establishing or Improving a Cybersecurity Program* are included [Bar+18]. The scope of the environment is analyzed and the criticality of the environment is identified. The criticality is how important the security of the environment is and what the degree of the related consequences are. This criticality implicates the maturity score the environment needs to be aligned to. The five different maturity levels of the Capability Maturity Model (CMM) are illustrated in table 6.1 [Pau+93]. In maturity assessments, regularly the CIA values are the benchmark. This research claims that the use of CFAM would be beneficial since this model is the most comprehensive model available. This should be included in the maturity score. This maturity score should be generated for each NIST category, serving as a maturity goal to which the environment must be aligned to secure the environment's criticality. A visualization of how these maturity goals are illustrated can be found in figure 6.1.

Secondly, the additions to the NIST framework are explained. These additions are structured in the same way as NIST. Therefore, the function and category are already given. The additional challenges that are identified for every category follow from the included frameworks and research. In the standards/solutions column, keywords and concepts are provided to

Maturity scale		
5	**Optimized**	Processes, systems, and training are systematically and continuously improved to increase efficiency and continuity.
4	**Managed**	Processes and systems are systematically managed and monitored, performance indicators have been defined, and trainings tailored to the needs.
3	**Defined**	Processes and systems are documented, monitored, maintained and managed in a consistent and repeatable manner, general trainings.
2	**Repeatable**	Repetitive processes and poorly documented, supported and managed, but not coherently, basic systems, ad-hoc trainings.
1	**Initial**	Ad-hoc processes, no description, repeatability, management, monitoring, training, or systems.

Table 6.1: *Maturity score based on the Capability Maturity Model [Pau+93].*

demonstrate what requires special attention in IoT-specific devices and environments. How these keywords and concepts can be interpreted, assessed, and improved, can be found in the attached references.

Thirdly, the outcome of the assessment framework. This is depending on the earlier identified maturity goal for every category. For every NIST category, the environment is checked on the IoT-specific standards and a maturity score is given to this category. This score is based on the CMM that considers CFAM. The current maturity score of the environment is mapped in the same way as the maturity goals were mapped. In combination, the current situation can be compared to the goal of the environment. A visualization of this mapping can be found in figure 6.4.

Finally, the outcome provides a score, based on the difference in quality between the current and the desired state. The categories that differ most from their desired state have the highest priority. When the distance between the current and the desired state decreases, the priority will also decrease. This assessment framework provides guidance based on the information in the frameworks and research results that are included. Here, the environments should strive to optimize the keywords and standards included in these previous works. Guidance should always be given in alignment with the PPT model [Sch01]. This is accounted for since the people will be guided by the adaptive and ethical challenges, the process by the operational and legal challenges, and the technologies by the technical challenges.

6.3 The assessment framework

The assessment framework starts with an elaborate environment assessment. In this assessment the worst-case scenario is imagined, focusing on the capacity of the devices, the scalability of the attack, and the data that is worked with. Based on the worst-case scenario, the criticality of the environment is defined. The criticality of the environment determines how secure the environment must strive to be. Therefore, based on the related consequences the criticality of every NIST category can be determined to create a maturity goal for this category. The environment assessment results in an overview of the state in which we meet our maturity goals. An illustration of an example desired state is given in figure 6.1.

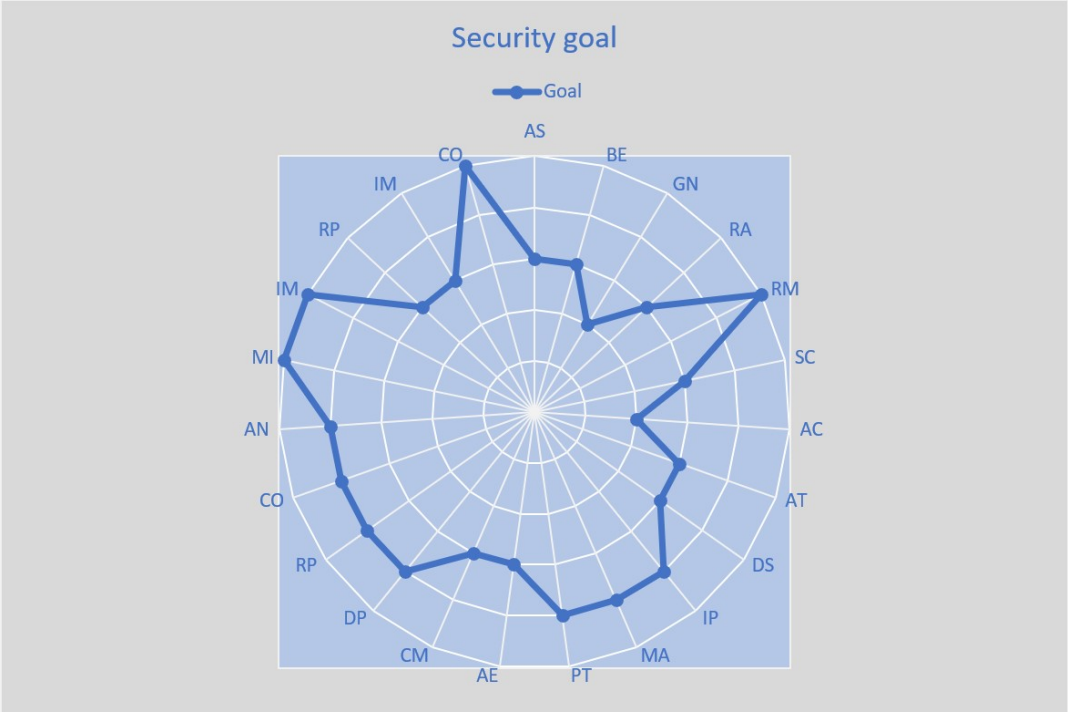

Figure 6.1: *Goal of the environment after the environment assessment.*

Figure 6.1 shows the maturity goals for every NIST category. This maturity is partly based on the currently available NIST framework [Bar+18]. Besides, the NIST framework is expanded with the IoT additions. These additions offer solutions to the identified challenges found in IoT-based environments. What challenges are related to the NIST categories is illustrated in figure 6.2. The framework that identified the keywords for standards and

solutions to these challenges can be found on the following pages.

FUNCTION	CATEGORY	CHALLENGES
ID. IDENTIFY	AM. Asset Management	Technical, legal, ethical, operational, and adaptive
	BE. Business Environment	Technical and operational
	GV. Governance	Technical, legal, ethical, operational, and adaptive
	RA. Risk Assessment	Technical, legal, ethical, operational, and adaptive
	RM. Risk Management Strategy	Technical, legal, ethical, operational, and adaptive
	SC. Supply Chain Risk Management	Technical, legal, ethical, operational, and adaptive
PR. PREDICT	AC. Identity Management and Access Control	Technical, legal, ethical, operational, and adaptive
	AT. Awareness and Training	Technical, legal, ethical, operational, and adaptive
	DS. Data Security	Technical, legal, ethical, operational, and adaptive
	IP. Information Protection Processes and Procedures	Technical, legal, ethical, operational, and adaptive
	MA. Maintenance	Technical, legal, ethical, operational, and adaptive
	PT. Protective Technology	Technical, legal, ethical, and operational
DT. DETECT	AE. Anomalies and Events	Technical, operational, and adaptive
	CM. Security Continuous Monitoring	Technical, legal, ethical, and operational
	DP. Detection Processes	Technical
RS. RESPOND	RP. Response Planning	Technical, operational, and adaptive
	CO. Communications	Technical, operational, and adaptive
	AN. Analysis	Technical
	MI. Mitigation	Technical, operational, and adaptive
	IM. Improvements	Technical, operational, and adaptive
RC. RECOVER	RP. Recovery Planning	Technical
	IM. Improvements	Technical
	CO. Communications	Technical and legal

Figure 6.2: *IoT challenges related to the NIST categories*

FUNCTION	CATEGORY	CHALLENGE	STANDARDS / SOLUTIONS	REFERENCES
ID	**ID.AM**	Technical	Authorization, cryptography, secure interfaces and network services, authentication, secure software updates, secure and trusted communications, secure input and output handling, hardware security, trust and integrity management, strong default security and privacy, third-party software, internal processing, segmentation and standardization, enforce minimal controls	ENISA baseline ENISA good practices IEC 62443-4-2:2019 Patel et al. (2016) Qiu et al. (2021)
		Legal	Security by design, asset management, risk and threats identification and assessment, vendor regulation, safe fail system	ENISA baseline ENISA IoT guidelines Karie et al. (2021) Lata and Kumar (2021)
		Ethical	Security by design, asset management, risk and threats identification and assessment,	ENISA baseline ENISA IoT guidelines Karie et al. (2021)
		Operational	Proven solutions, management of security vulnerabilities, hardware threats, segmentation and standardization, enforce minimal controls, security analytics	ENISA baseline IEC 62443-4-1:2018 Aboelfotoh & Hikal (2019) Patel et al. (2016) Karie et al. (2021)
		Adaptive	Proven solutions, management of security vulnerabilities	ENISA baseline
	ID.BE	Technical	Device operating system, mobile application, secure supply chain and production	IOTSF 2.4.6, 2.4.11, 2.4.14
		Operational	Device operating system, secure supply chain and production, third-party management	ENISA good practices IOTSF 2.4.6, 2.4.14
	ID.GV	Technical	Data protection and compliance, secure software updates, authentication, monitoring and auditing, access control: physical and environmental security, secure interfaces and network services, secure input and output handling, strong default security and privacy, device ownership transfer, enforce minimal controls	ENISA baseline IOTSF 2.4.16 Patel et al. (2016)
		Legal	Privacy by design, risk and threats identification and assessment, security by design, business security processes, policies and	ENISA baseline ENISA IoT guidelines IOTSF 2.4.3, 2.4.16 Karie et al. (2021) Lata and Kumar (2021)

			responsibilities, device ownership transfer, vendor regulation	
		Ethical	Privacy by design, risk and threats identification and assessment, security by design, business security processes, policies and responsibilities	ENISA baseline ENISA IoT guidelines IOTSF 2.4.3 Karie et al. (2021)
		Operational	Third-party relationships, human resource security training and awareness, business security processes, policies and responsibilities, device ownership transfer, countermeasures, basic cyber hygiene, enforce minimal controls, patching, security analytics	ENISA baseline IEC 62443-4-1:2018 IOTSF 2.4.3, 2.4.16 Aboelfotoh & Hikal (2019) Patel et al. (2016) Karie et al. (2020) Karie et al. (2021)
		Adaptive	Third-party relationships, human resource security training and awareness	ENISA baseline
	ID.RA	Technical	Secure interfaces and network services, data protection and compliance, monitoring and auditing, access control: physical and environmental security, strong default security and privacy, vulnerabilities, segmentation and standardization, threat landscape and boundary defense, DDoS mitigation	ENISA baseline Aboelfotoh & Hikal (2019) Patel et al. (2016) Karie et al. (2020) Qiu et al. (2021)
		Legal	Privacy by design, risk and threats identification and assessment, security by design, safe fail system	ENISA baseline ENISA IoT guidelines Karie et al. (2021)
		Ethical	Privacy by design, risk and threats identification and assessment, security by design	ENISA baseline ENISA IoT guidelines Karie et al. (2021)
		Operational	Third-party relationships, human resource security training and awareness, security design, natural threats, segmentation and standardization	ENISA baseline ENISA good practices IEC 62443-4-1:2018 Aboelfotoh & Hikal (2019) Patel et al. (2016)
		Adaptive	Third-party relationships, human resource security training and awareness	ENISA baseline
	ID.RM	Technical	Secure interfaces and network services, data protection and compliance, monitoring and auditing, access control: physical and environmental security, strong default security and	ENISA baseline Aboelfotoh & Hikal (2019) Patel et al. (2016)

			privacy, penetration testing, segmentation and standardization, enforce minimal controls	
		Legal	Privacy by design, risk and threats identification and assessment, security by design	ENISA baseline ENISA IoT guidelines Karie et al. (2021)
		Ethical	Privacy by design, risk and threats identification and assessment, security by design	ENISA baseline ENISA IoT guidelines Karie et al. (2021)
		Operational	Third-party relationships, human resource security training and awareness, security design, data mitigation, basic cyber hygiene, segmentation and standardization, enforce minimal controls, trusted anchors and attestation	ENISA baseline ENISA good practices IEC 62443-4-1:2018 Hughes & Cybenko (2013) Patel et al. (2016)
		Adaptive	Third-party relationships, human resource security training and awareness	ENISA baseline
	ID.SC	Technical	Secure supply chain and production, enforce minimal controls	IEC 62443-4-2:2019 IOTSF 2.4.14 Patel et al. (2016)
		Legal	Leverage existing standards and good practices, forging better relationships between actors, vendor regulation	ENISA IoT guidelines Lata and Kumar (2021)
		Ethical	Security by design	ENISA IoT guidelines Karie et al. (2021)
		Operational	Secure supply chain and production, third-party management, comprehensive and explicit approach to security, security by design, enforce minimal controls, hardware testing	ENISA good practices ENISA IoT guidelines IEC 62443-4-1:2018 IOTSF 2.4.14 Patel et al. (2016) Karie et al. (2021)
		Adaptive	Cybersecurity expertise should be further cultivated	ENISA IoT guidelines
PR	**PR.AC**	Technical	Authorization, authentication, secure software updates, system safety and reliability, access control: physical and environmental security, strong default security and privacy, secure interfaces and network services, hardware security, secure and trusted communication, trust and integrity management, device wired and wireless interfaces,	ENISA baseline IEC 62443-4-2:2019 IOTSF 2.4.7, 2.4.8, 2.4.13 Aboelfotoh & Hikal (2019) Patel et al. (2016)

			cloud and network elements, segmentation and standardization	
		Legal	Security by design, device wired and wireless interfaces, end-to-end credentials	ENISA baseline ENISA IoT guidelines IOTSF 2.4.7 Karie et al. (2021)
		Ethical	Security by design	ENISA baseline ENISA IoT guidelines Karie et al. (2021)
		Operational	End-of-life support, device wired and wireless interfaces, authorization, authentication, cloud and network elements, SLDC methodology, segmentation and standardization	ENISA baseline ENISA good practices IEC 62443-4-1:2018 IOTSF 2.4.7, 2.4.13 Patel et al. (2016)
		Adaptive	End-of-life support	ENISA baseline
	PR.AT	Technical	Data protection and compliance, monitoring and auditing, access control: physical and environmental security, secure interfaces and network services, strong default security and privacy	ENISA baseline ENISA good practices
		Legal	Privacy by design, risk and threats identification and assessment	ENISA baseline
		Ethical	Privacy by design, risk and threats identification and assessment, roles and privileges, humans	ENISA baseline ENISA good practices Aboelfotoh & Hikal (2019)
		Operational	Third-party relationships, human resource security training and awareness, cybersecurity expertise further cultivated	ENISA baseline ENISA good practices ENISA IoT guidelines Schneier (2000)
		Adaptive	Third-party relationships, human resource security training and awareness, security culture	ENISA baseline ENISA good practices ENISA IoT guidelines
	PR.DS	Technical	Authorization, cryptography, secure interfaces and network services, authentication, secure software updates, secure and trusted communications, secure input and output handling, hardware security, trust and integrity management, strong default security and privacy, physical security, device software, encryption and key management for hardware, web user interface, data protection	ENISA baseline IOTSF 2.4.4, 2.4.5, 2.4.9, 2.4.10, 2.4.12, 2.4.16 Patel et al. (2016) Karie et al. (2021)

			and privacy, device ownership transfer, API security	
		Legal	Security by design, asset management, risk and threats identification and assessment, device software, encryption and key management for hardware, web user interface, data protection and privacy, device ownership transfer	ENISA baseline ENISA IoT guidelines IOTSF 2.4.5, 2.4.9, 2.4.10, 2.4.12, 2.4.16 Patel et al. (2016) Karie et al. (2021)
		Ethical	Security by design, asset management, risk and threats identification and assessment, privacy protection	ENISA baseline ENISA IoT guidelines Patel et al. (2016) Karie et al. (2021)
		Operational	Proven solutions, management of security vulnerabilities, device software, encryption and key, data protection and privacy management for hardware, web user interface, device ownership transfer	ENISA baseline IEC 62443-4-1:2018 IOTSF 2.4.5, 2.4.9, 2.4.10, 2.4.12, 2.4.16 Aboelfotoh & Hikal (2019) Karie et al. (2021)
		Adaptive	Proven solutions, management of security vulnerabilities	ENISA baseline
	PR.IP	Technical	Authorization, cryptography, secure interfaces and network services, authentication, secure software updates, secure and trusted communications, secure input and output handling, hardware security, trust and integrity management, strong default security and privacy, device operating system, cloud and network elements, vulnerabilities, API security	ENISA baseline ENISA good practices IOTSF 2.4.6, 2.4.13 Aboelfotoh & Hikal (2019) Patel et al. (2016) Karie et al. (2021)
		Legal	Security by design, asset management, risk and threats identification and assessment, privacy protection	ENISA baseline ENISA IoT guidelines Patel et al. (2016) Karie et al. (2021)
		Ethical	Security by design, asset management, risk and threats identification and assessment, humans, privacy protection	ENISA baseline ENISA IoT guidelines Aboelfotoh & Hikal (2019) Patel et al. (2016) Karie et al. (2021)
		Operational	Proven solutions, management of security vulnerabilities, device operating system, cloud and network elements, configuration, secure deployment, internal policies, policies, countermeasures, data	ENISA baseline ENISA good practices IEC 62443-4-1:2018 IOTSF 2.4.6, 2.4.13, 2.4.15 Aboelfotoh & Hikal (2019) Hughes & Cybenko (2013) Patel et al. (2016)

			mitigation, trusted anchors and attestation	
		Adaptive	Proven solutions, management of security vulnerabilities	ENISA baseline
	PR.MA	Technical	Secure software updates, system safety and reliability, monitoring and auditing, trust and integrity management, enforce minimal controls	ENISA baseline IEC 62443-4-2:2019 Patel et al. (2016)
		Legal	Security by design, vendor regulation	ENISA baseline ENISA IoT guidelines Karie et al. (2021) Lata and Kumar (2021)
		Ethical	Security by design	ENISA baseline ENISA IoT guidelines Karie et al. (2021)
		Operational	Management of security vulnerabilities, end-of-life support, basic cyber hygiene, enforce minimal controls, hardware testing, patching	ENISA baseline IEC 62443-4-1:2018 Patel et al. (2016) Karie et al. (2020) Karie et al. (2021)
		Adaptive	Management of security vulnerabilities, end-of-life support	ENISA baseline
	PR.PT	Technical	Secure interfaces and network services, secure and trusted communications, trust and integrity management, cloud and network elements, secure code, secure sensor interaction, threat landscape and boundary defense, blockchain, API security, safe fail system	ENISA baseline ENISA good practices IOTSF 2.4.13 Aboelfotoh & Hikal (2019) Patel et al. (2016) Karie et al. (2020) Karie et al. (2021) Reyna et al. (2018) Qiu et al. (2021)
		Legal	Security by design	ENISA baseline ENISA IoT guidelines Karie et al. (2021)
		Ethical	Security by design	ENISA baseline ENISA IoT guidelines Karie et al. (2021)
		Operational	Cloud and network elements, configuration, policies, countermeasures	IEC 62443-4-1:2018 IOTSF 2.4.13, 2.4.15 Aboelfotoh & Hikal (2019)
DT	**DT.AE**	Technical	System safety and reliability, logging, monitoring and auditing, trust and integrity management, cloud and network elements, secure implementation, virus detection	ENISA baseline ENISA good practices IOTSF 2.4.13 Aboelfotoh & Hikal (2019)
		Operational	Management of security vulnerabilities, cloud and network	ENISA baseline ENISA good practices IOTSF 2.4.13

			elements, operations management	
		Adaptive	Management of security vulnerabilities	ENISA baseline
	DT.CM	Technical	System safety and reliability, logging, access control: physical and environmental security, monitor and auditing, hardware security, trust and integrity management, device software, device wired and wireless interfaces, cloud and network elements, security reviews, vulnerabilities, virus detection, penetration testing, IDS	ENISA baseline ENISA good practices IEC 62443-4-2:2019 IOTSF 2.4.5, 2.4.7, 2.4.13 Aboelfotoh & Hikal (2019) Karie et al. (2020)
		Legal	Security by design, device software, device wired and wireless interfaces	ENISA baseline ENISA IoT guidelines IOTSF 2.4.5, 2.4.7 Karie et al. (2021)
		Ethical	Security by design	ENISA baseline ENISA IoT guidelines Karie et al. (2021)
		Operational	device software, device wired and wireless interfaces, cloud and network elements, device monitoring, security analytics	IEC 62443-4-1:2018 IOTSF 2.4.5, 2.4.7, 2.4.13 Karie et al. (2021)
	DT.DP	Technical	Logging, monitoring and auditing, security of SDLC infrastructure, network, virus detection, penetration testing, secure sensor interaction, IDS	ENISA baseline ENISA good practices Aboelfotoh & Hikal (2019) Patel et al. (2016) Karie et al. (2020)
RS	**RS.RP**	Technical	System safety and reliability, logging, monitoring and auditing, trust and integrity management, safe fail system	ENISA baseline Qiu et al. (2021)
		Operational	Management of security vulnerabilities	ENISA baseline
		Adaptive	Management of security vulnerabilities	ENISA baseline
	RS.CO	Technical	System safety and reliability, logging, monitoring and auditing, trust and integrity management	ENISA baseline
		Operational	Management of security vulnerabilities	ENISA baseline
		Adaptive	Management of security vulnerabilities	ENISA baseline
	RS.AN	Technical	System safety and reliability, logging, monitoring and auditing, trust and integrity management	ENISA baseline
	RS.MI	Technical	System safety and reliability, logging, monitoring and auditing,	ENISA baseline Karie et al. (2020)

			trust and integrity management, DDoS mitigation	
		Operational	Management of security vulnerabilities	ENISA baseline
		Adaptive	Management of security vulnerabilities	ENISA baseline
	RS.IM	Technical	System safety and reliability, logging, monitoring and auditing, trust and integrity management	ENISA baseline
		Operational	Management of security vulnerabilities	ENISA baseline
		Adaptive	Management of security vulnerabilities	ENISA baseline
RC	**RC.RP**	Technical	Trust and integrity management, system safety and reliability	ENISA baseline
	RC.IM	Technical	Trust and integrity management, system safety and reliability	ENISA baseline
	RC.CO	Technical	Trust and integrity management, system safety and reliability	ENISA baseline
		Legal	Vendor regulation	Lata and Kumar (2021)

Figure 6.3: *Core of the cybersecurity assessment framework for IoT-based environments*

The assessment framework provides guidance to assess an environment. With the help of the keywords and the explanations in the references, the framework can assess IoT-based environments. Just like how NIST is practiced this assessment framework provides a certain score depending on the assessment of the security level of additional IoT categories. This will be aligned into a maturity score for every single category. These values will be mapped to the original goal of the environment. A visualization of this can be found in figure 6.4.

The final score that the IoT-based environment receives is based on the distance between the two states. This outcome prioritizes the categories that are most distant from their desired state. How to increase the security for these categories can be found in the references associated with this category, the CMM, and the CFAM.

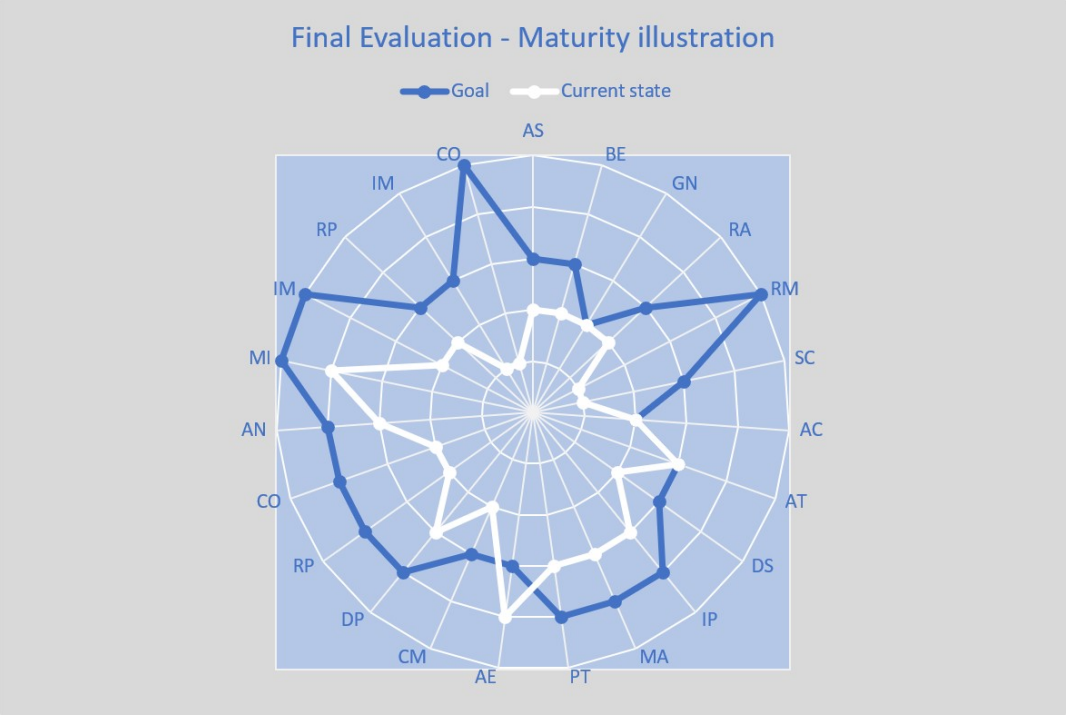

Figure 6.4: *Final evaluation of the environment.*

6.4 Framework evaluation

In the previous section, the final assessment framework was presented. This section will evaluate this assessment framework, by making a summary of the discussion and design section and elaborating on the implementation. Therefore , this section will propose the (dis)advantages of the assessment framework and its relation to other frameworks.

There are various reasons why this format is chosen for the assessment framework. To evaluate this motivation, the advantages are discussed. First of all, the NIST cybersecurity framework is chosen as a baseline due to its advantages. NIST is a large institute that has a lot of expertise in cybersecurity. In addition, the structure of the NIST framework provides dynamic elements that lead to more security over time with the help of the subsequent processes: identifying, protecting, detecting, responding, and recovering. Furthermore, the comprehensiveness of the framework is considered high and the transition costs for IoT-based environments will be low as they will most likely already have worked with NIST earlier. The final advantage of NIST is that it already covers IT and OT. This makes IoT the only thing

that needs to be added to the framework to be comprehensive. Together, NIST provides numerous advantages and is therefore used as a baseline.

Second, the advantage of including ENISA, IEC, IoTSF, and the previously discussed research in the assessment framework. These frameworks were identified as useful frameworks in practice. In addition, the previously discussed research showed to add value in the literature review of this research. Therefore, all these sources are considered relevant to add to the NIST baseline.

Third, is the advantage that the chosen structure brings. This structure provides the ability to align the environment assessment to the maturity score and make the whole assessment bound and linked. In addition, this structure provided the ability to give the feedback and guidance that is expected from an assessment framework. To sum up, the choices made in the structure of this assessment framework provide a lot of advantages.

On the other hand, there are also some limitations to this assessment framework and they are related to its readiness for implementation. Several previously identified challenges could not yet be covered by the framework's chosen implementation. The first limitation is that the framework is not complete, it does not cover all IoT limitations, and certainly not all useful research. This means that in the coming time this framework should be elaborated to become more comprehensive and complete. This can happen by mapping more relevant work to specific IoT problems. The second limitation of the framework is that it is not yet tested and validated by experts to ensure its applicability. A framework needs to be applicable to be of value [Eld+06]. The third limitation is the lack of descriptive outcomes. This was identified to be valuable as it provides more insights into the environment. In addition, things as KPIs and KRIs can be implemented as useful tools to make the framework more dynamic. However, more research is needed to know what should be included in this descriptive feedback. The fourth limitation is that the included security levels and the quantitative metrics are outsourced to the included frameworks and research. This makes the inclusion of all security levels fully dependent on what these frameworks and researches provide. The last limitation of the framework is the inability to cover regulatory challenges. These challenges are the most important in the journey towards safe environments but must be solved by the regulators. This framework proposes key concepts regulators need to focus on in improving the security of IoT-based environments. Thus, there is a lot of room

to improve the quality of this assessment framework. Therefore, more research and work is needed to finish the assessment framework.

The generated assessment framework has a lot of advantages but also still faces limitations. However, the assessment framework is certainly adding value to the academic field of IoT security. Currently, the most important cybersecurity assessment frameworks fail to identify the five main IoT challenges (technical, legal, ethical, operational, and adaptive) [Kar+21]. In addition, the security standards have little focus on IoT-specific devices. The research and frameworks that do focus on IoT specifically are often only proposing single good practices but are not translated to assessment frameworks. This research translates good practices into an assessment framework for IoT-based environments, and the translation from an IoT-specific assessment framework towards an IT, OT, and IoT converged cybersecurity assessment framework that can be applied to all environments including embedded devices.

Chapter 7

Conclusion

This research is designed to answer the following main research question: *"How to assess challenges and differences in the security of IoT-based environments, compared to the security of traditional computing devices?"* An assessment framework is necessary to be able to provide security to IoT-based environments [Kar+21]. This is a massive challenge considering the rapid growth of IoT [Jov21]. As shown in figure 7.1, to answer this main research question a cybersecurity assessment framework for IoT-based environments is proposed. This assessment framework could be generated after answering five consecutive subquestions.

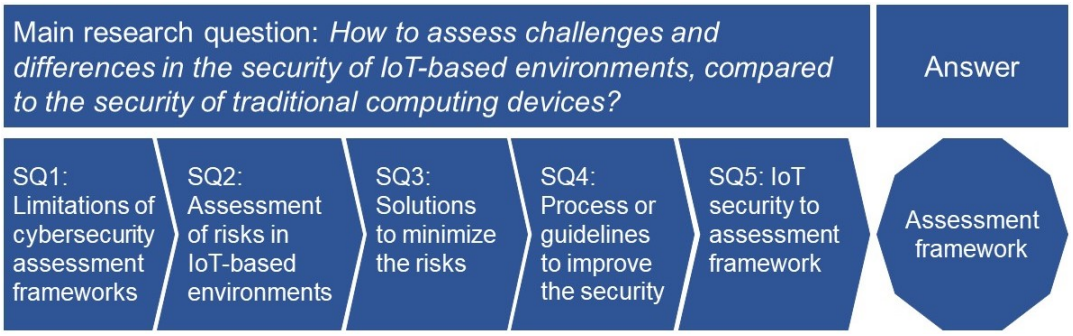

Figure 7.1: *Overview of how this research is structured.*

SQ1: What are the limitations of the available cybersecurity assessment frameworks for IoT-based environments?

The current frameworks consequently fail to meet four challenges. First, the comprehensiveness of the overall framework is a challenge. Frameworks

often exclude very important steps in the assessment of an environment. Second, the comprehensiveness of the assessment method is a challenge. Frameworks consist of multiple sub-assessments, these sub-assessments individually need to provide all the relevant outcomes, and frameworks often fail to identify these. Third, IoT-specific challenges are often neglected. IoT-specific challenges can be structured into five subcategories: technical-, legal-, ethical-, operational-, and adaptive challenges [Kar+21]. Last, the applicability of the framework is often neglected [Les21]. However, a assessment framework must be applicable to have value.

SQ2: How can risks in IoT-based environments be assessed?

The first subquestion identified 4 different challenges to assess. The first two challenges were solved by the interviews. These identified what needs to be included to provide a comprehensive assessment framework and comprehensive assessment method. Furthermore, the five main challenges should be assessed in similar ways as existing challenges are being assessed [NIS11]. In this assessment, the best practice should be based upon. In addition, the applicability of the assessment framework should be validated by experts, based on the 8 points of Eldh et al. [Eld+06].

SQ3: What are potential solutions to minimize the risks in IoT-based environments?

To make sure that the assessment framework can guide IoT-based environments to improve their security, solutions to the challenges are needed. The range of solutions is very broad and every individual solution focuses on another IoT challenge. The identified solutions were retrieved from research, interviews, and existing IoT security frameworks. The useful IoT security frameworks are created by ENISA, IEC, and IoTSF [Gin+17; Com18; WG121].

SQ4: What overall process or guidelines can be implemented to improve the security of IoT-based environments?

A good practice for a new assessment framework is to base it upon existing best practice frameworks [Ali+20]. The outcome of this research is that the NIST cybersecurity framework should be used as a baseline. To provide this framework with more specific IoT guidance the solutions of the ENISA, IEC 62443, and IoTSF are combined with the solutions found in the data and interviews. The implementation of this list of good practices would guide IoT-based environments to improve their security.

SQ5: How can the IoT-based environment security be generalized into an overall applicable assessment framework?

All the solutions that are generated in subquestion 4 can be listed and mapped according to the categories in the NIST framework. To provide more structure and guidance, these solutions are divided into the 5 main IoT challenges (technical, legal, ethical, operational, and ethical) [Kar+21]. With the addition of an environment- and maturity assessment, the assessment framework becomes able to provide the desirable guidance.

Together, the generated assessment framework has a lot of advantages but also faces limitations that are related to the applicability of the assessment framework. However, the assessment framework does add value to the academic field of IoT security. Currently, the cybersecurity assessment frameworks fail to identify the five main IoT challenges and the security standards have little focus on IoT-specific devices [Kar+21]. The existing IoT-based research and frameworks only propose single good practices but do not translate these best practices to an assessment framework. Therefore, it is very valuable that this research has translated good practices into an assessment framework. Finally, another valuable outcome of this research has been that a step was made toward a cybersecurity assessment framework that includes IT, OT, and IoT, that can be applied to all environments including embedded devices. This chose is made since it is better to improve current assessment frameworks and converge and expand them with IoT challenges than to create a specific assessment framework for IoT-based environments.

7.1 Future research

Apart from the value that the assessment framework generates, some limitations could not be covered. The first limitation is that the assessment framework is not complete yet. Not all relevant frameworks, nor all research could be included in this assessment framework. This implies that more references can be added to the assessment framework to generate more value. Second, the applicability of the assessment framework is not yet validated. This step is necessary to illustrate the value and the way to interpret the assessment framework. Third, the relevant descriptive outcomes are not included since more research is needed on what values are relevant. Fourth, the coverage of different security levels is currently completely outsourced. To make sure the different security levels are included, the information of the references in the

assessment framework should be written out completely to determine the different levels. The last limitation is that the assessment framework is unable to cover regulatory challenges. These challenges are the most important in the journey towards safe IoT-based environments but for the assessment framework itself, the regulations in place are a given. Therefore, the regulatory challenges must be solved by the regulators. Future research should provide answers to these five limitations of the assessment framework to make it more applicable.

Bibliography

[SC90] Anselm Strauss and Juliet Corbin. *Basics of qualitative research*. Sage publications, 1990.

[Pau+93] Mark C Paulk et al. "Capability maturity model, version 1.1." In: *IEEE software* 10.4 (1993), pp. 18–27.

[Bal+95] Hari Balakrishnan et al. "Improving TCP/IP performance over wireless networks." In: *Proceedings of the 1st annual international conference on Mobile computing and networking*. 1995, pp. 2–11.

[JJ98] Neil F Johnson and Sushil Jajodia. "Exploring steganography: Seeing the unseen." In: *Computer* 31.2 (1998), pp. 26–34.

[SC98] Anselm Strauss and Juliet Corbin. "Basics of qualitative research techniques." In: (1998).

[LL00] Michael R Lyu and Lorrien KY Lau. "Firewall security: Policies, testing and performance evaluation." In: *Proceedings 24th Annual International Computer Software and Applications Conference. COMPSAC2000*. IEEE. 2000, pp. 116–121.

[Sch00] B Schneier. *Secrets and Lies: Security in a Digital World*. 2000.

[Sch01] Steven Schlarman. "The people, policy, technology (PPT) model: core elements of the security process." In: *Information systems security* 10.5 (2001), pp. 1–6.

[VM01] John Viega and Gary R McGraw. *Building secure software: How to avoid security problems the right way, portable documents*. Pearson Education, 2001.

[Zha+04] Zhensheng Zhang et al. "An overview of virtual private network (VPN): IP VPN and optical VPN." In: *Photonic network communications* 7.3 (2004), pp. 213–225.

[Pol05] Donald E Polkinghorne. "Language and meaning: Data collection in qualitative research." In: *Journal of counseling psychology* 52.2 (2005), p. 137.

[CG06] Juan Chen and Chuanxiong Guo. "Online detection and prevention of phishing attacks." In: *2006 First International Conference on Communications and Networking in China*. IEEE. 2006, pp. 1–7.

[Eld+06] Sigrid Eldh et al. "A framework for comparing efficiency, effectiveness and applicability of software testing techniques." In: *Testing: Academic & Industrial Conference-Practice And Research Techniques (TAIC PART'06)*. IEEE. 2006, pp. 159–170.

[McI06] Angus McIlwraith. *Information security and employee behaviour how to reduce risk through employee education, training and awareness*. eng. Aldershot, England ; Burlington, VT: Gower, 2006. ISBN: 1-317-11674-7.

[Par+06] Lydia Parziale et al. "TCP/IP tutorial and technical overview." In: (2006).

[SHB06] Marianne Swanson, J Hash, and P Bowen. "NIST Special Publication 800-18 Revision 1." In: *Guide for Developing Security Plans for Federal Information Systems* (2006).

[VY06] Amit Vasudevan and Ramesh Yerraballi. "Spike: engineering malware analysis tools using unobtrusive binary-instrumentation." In: *Proceedings of the 29th Australasian Computer Science Conference-Volume 48*. Citeseer. 2006, pp. 311–320.

[Boe08] Wolfgang Boehmer. "Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001." In: *2008 Second International Conference on Emerging Security Information, Systems and Technologies*. IEEE. 2008, pp. 224–231.

[Fen08] Kim Fenrich. "Securing your control system: the "CIA triad" is a widely used benchmark for evaluating information system security effectiveness." eng. In: *Power engineering (Barrington, Ill.)* 112.2 (2008), p. 44. ISSN: 0032-5961.

[Jan08] Irving L Janis. "Groupthink." In: *IEEE Engineering Management Review* 36.1 (2008), p. 36.

[LK08] Younghwa Lee and Kenneth A Kozar. "An empirical investigation of anti-spyware software adoption: A multitheoretical perspective." eng. In: *Information management* 45.2 (2008), pp. 109–119. ISSN: 0378-7206.

[Onl09] Grounded Theory Online. *What is Grounded Theory?* https://www.groundedtheoryonline.com/what-is-grounded-theory/. [Accessed: 2022-16-03]. 2009.

[ZM09] Lixuan Zhang and William C McDowell. "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords." eng. In: *Journal of Internet commerce* 8.3-4 (2009), pp. 180–197. ISSN: 1533-2861.

[Dar10] Glenn S Dardick. "Cyber forensics assurance." In: (2010).

[VZS10] Antonio J Jara Valera, Miguel A Zamora, and Antonio FG Skarmeta. "An architecture based on internet of things to support mobility and security in medical environments." In: *2010 7th IEEE consumer communications and networking conference*. IEEE. 2010, pp. 1–5.

[Zho+10] Wu Zhou et al. "Always up-to-date: scalable offline patching of vm images in a compute cloud." In: *Proceedings of the 26th Annual Computer Security Applications Conference*. 2010, pp. 377–386.

[AG11] Asmaa Shaker Ashoor and Sharad Gore. "Importance of intrusion detection system (IDS)." In: *International Journal of Scientific and Engineering Research* 2.1 (2011), pp. 1–4.

[Hou11] Congress House of Representatives. *United States Code, 44 U.S.C. 3542 - Definitions*. https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542. [Accessed: 2022-02-03]. 2011.

[NIS11] NIST. *NIST SP 80039 Managing Information Security Risk Organization, Mission, and Information System View*. Technical Report March. 2011.

[RH11] Helena Rifa-Pous and Jordi Herrera-Joancomartí. "Computational and energy costs of cryptographic algorithms on handheld devices." In: *Future internet* 3.1 (2011), pp. 31–48.

[SD11] Kevin Stine and Quynh Dang. "Encryption basics." In: *Journal of AHIMA* 82.5 (2011), pp. 44–46.

[Mat+12] Mark Mateski et al. "Cyber threat metrics." In: *Sandia National Laboratories* (2012), p. 30.

[SN12] National Institute of Standards and Technology (NIST). *Guide for Conducting Risk Assessments SP-800-30 â Revision 1*. https://doi.org/10.6028/NIST.SP.800-30r1. 2012.

[Col13] Eric Cole. "Chapter 1 - The Changing Threat." In: *Advanced Persistent Threat*. Ed. by Eric Cole. Boston: Syngress, 2013, pp. 3–26. ISBN: 978-1-59749-949-1. DOI: https://doi.org/10.1016/B978-1-59-749949-1.00001-2.

[De +13] Emiliano De Cristofaro et al. "A comparative usability study of two-factor authentication." In: *arXiv preprint arXiv:1309.5344* (2013).

[Gub+13] Jayavardhana Gubbi et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." In: *Future generation computer systems* 29.7 (2013), pp. 1645–1660.

[HC13] Jeff Hughes and George Cybenko. "Quantitative metrics and risk assessment: The three tenets model of cybersecurity." In: *Technology Innovation Management Review* 3.8 (2013).

[Lia+13] Hung-Jen Liao et al. "Intrusion detection system: A comprehensive review." In: *Journal of Network and Computer Applications* 36.1 (2013), pp. 16–24.

[VV13] Rossouw Von Solms and Johan Van Niekerk. "From information security to cyber security." In: *computers & security* 38 (2013), pp. 97–102.

[Cam14] Suzanne Campbell. "What is qualitative research?" In: *Clinical Laboratory Science* 27.1 (2014), p. 3.

[Jam14] Shazia Jamshed. "Qualitative research method-interviewing and observation." In: *Journal of basic and clinical pharmacy* 5.4 (2014), p. 87.

[JRT14] Roksana Janghorban, Robab Latifnejad Roudsari, and Ali Taghipour. "Skype interviewing: The new generation of online synchronous interview in qualitative research." In: *International journal of qualitative studies on health and well-being* 9.1 (2014), p. 24152.

[SR14] Marco Spruit and Martijn Röling. "ISFAM: the information security focus area maturity model." In: (2014).

[CSH15] Amanda N Craig, Scott J Shackelford, and Janine S Hiller. "Proactive cybersecurity: A comparative industry and regulatory analysis." In: *American Business Law Journal* 52.4 (2015), pp. 721–787.

[CV+15] Ivan Cvitić, Miroslav Vujić, et al. "CLASSIFICATION OF SECURITY RISKS IN THE IOT ENVIRONMENT." In: *Annals of DAAAM & Proceedings* 26.1 (2015).

[DiM+15] Daniel DiMase et al. "Systems engineering framework for cyber physical security and resilience." In: *Environment Systems and Decisions* 35.2 (2015), pp. 291–300.

[LOW15] JULIE LOWRIE. "A Primer of US and International Legal Aspects." In: *CYBERSECURITY* (2015), p. 199.

[Szm15] Maciej Szmit. "Security Management and Risk Management Approach in Cybersecurity and Information Security Management." In: *Medzinárodná vedecká konferencia Riešenie krízovỳch situácií v špecifickom prostredí, Fakulta bezpečnostného inžinierstva ŽU, Žilina* 20.21 (2015), pp. 651–656.

[Tro15] Tatiana Tropina. "Public–private collaboration: Cybercrime, cybersecurity and national security." In: *Self-and co-regulation in Cybercrime, cybersecurity and national security*. Springer, 2015, pp. 1–41.

[CP16] John W Creswell and Cheryl N Poth. *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications, 2016.

[OBr16] Ralph O'Brien. "Privacy and security: The new European data protection regulation and it's data breach notification requirements." In: *Business Information Review* 33.2 (2016), pp. 81–84. DOI: 10.1177/0266382116650297.

[Off16] Publications Office. *REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. [Accessed: 2022-02-01]. 2016.

[PP+16] Keyur K Patel, Sunil M Patel, et al. "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges." In: *International journal of engineering science and computing* 6.5 (2016).

[Ran+16] Alireza Ranjbar et al. "An SDN-based approach to enhance the end-to-end security: SSL/TLS case study." In: *NOMS 2016-2016 IEEE/IFIP network operations and management symposium*. IEEE. 2016, pp. 281–288.

[SSA16] Zahoor Ahmed Soomro, Mahmood Hussain Shah, and Javed Ahmed. "Information security management needs more holistic approach: A literature review." In: *International Journal of Information Management* 36.2 (2016), pp. 215–225.

[WH16] Lanier Watkins and John S Hurley. "The next generation of scientific-based risk metrics: measuring cyber maturity." In: *International Journal of Cyber Warfare and Terrorism (IJCWT)* 6.3 (2016), pp. 43–52.

[AR17] Adel Alkhalil and Rabie A. Ramadan. "IoT Data Provenance Implementation Challenges." In: *Procedia Computer Science* 109 (2017). 8th International Conference on Ambient Systems, Networks and Technologies, ANT-2017 and the 7th International Conference on Sustainable Energy Information Technology, SEIT 2017, 16-19 May 2017, Madeira, Portugal, pp. 1134–1139. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2017.05.436.

[Gin+17] Anibal Gines et al. *Baseline Security Recommendations for IoT*. Nov. 2017. URL: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[Liu+17] Yining Liu et al. "A secure data backup scheme using multi-factor authentication." eng. In: *IET information security* 11.5 (2017), pp. 250–255. ISSN: 1751-8709.

[NCD17] Jason RC Nurse, Sadie Creese, and David De Roure. "Security risk assessment in Internet of Things systems." In: *IT professional* 19.5 (2017), pp. 20–26.

[Sab+17] Regner Sabillon et al. "A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)." In: *2017 International Conference on Information Systems and Computer Science (INCISCOS)*. IEEE. 2017, pp. 253–259.

[Sin+17] Preeti Sinha et al. "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey." In: *2017 International Conference on Signal Processing and Communication (ICSPC)*. IEEE. 2017, pp. 288–293.

[Tos17] Okamura Toshihiko. "Lightweight cryptography applicable to various IoT devices." In: *NEC Technical Journal* 12.1 (2017), pp. 67–71.

[Bar+18] Matthew P Barrett et al. "Framework for improving critical infrastructure cybersecurity version 1.1." In: (2018).

[BSE18] Daniel Bastos, Mark Shackleton, and Fadiali El-Moussa. "Internet of things: A survey of technologies and security risks in smart home and city environments." In: (2018).

[Com18] Internation Electrotechnical Commission. *IEC 62443 2009-2018. IEC 62443 Security for Industrial Automation and Control Systems. Standard*. 2018.

[Del18] Deloitte. *Secure IoT by design*. https://www2.deloitte.com/us/en/pages/operations/articles/iot-platform-security.html. [Accessed: 2022-01-24]. Oct. 2018.

[Dix+18] Pooja Dixit et al. "Traditional and hybrid encryption techniques: a survey." In: *Networking communication and data knowledge engineering*. Springer, 2018, pp. 239–248.

[EAH18] Mohamed Faisal Elrawy, Ali Ismail Awad, and Hesham FA Hamed. "Intrusion detection systems for IoT-based smart environments: a survey." In: *Journal of Cloud Computing* 7.1 (2018), pp. 1–20.

[GBB18] Pradyumna Gokhale, Omkar Bhat, and Sagar Bhat. "Introduction to IOT." In: *International Advanced Research Journal in Science, Engineering and Technology* 5.1 (2018), pp. 41–44.

[KS18] Minhaj Ahmad Khan and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." In: *Future generation computer systems* 82 (2018), pp. 395–411.

[Kre18] Janine Kremling. *Cyberspace, cybersecurity, and cybercrime*. eng. 2018. ISBN: 9781506347257.

[Nur+18] Jason RC Nurse et al. "If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems." In: (2018).

[PRC18] Deepak Puthal, Rajiv Ranjan, and Jinjun Chen. "Big Data Stream Security Classification for IoT Applications." In: *Encyclopedia of Big Data Technologies*. Ed. by Sherif Sakr and Albert Zomaya. Cham: Springer International Publishing, 2018, pp. 1–5. ISBN: 978-3-319-63962-8. DOI: 10.1007/978-3-319-63962-8_236-1.

[Rey+18] Ana Reyna et al. "On blockchain and its integration with IoT. Challenges and opportunities." In: *Future generation computer systems* 88 (2018), pp. 173–190.

[Sen18] California Senate. *The California IoT cybersecurity law*. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327. [Accessed: 2022-02-17]. Sept. 2018.

[WJ18] Muchelule Yusuf Wanjala and Neyole Misiko Jacob. "Review of Viruses and Antivirus patterns." In: *Global Journal of Computer Science and Technology* (2018).

[AH19] Said F Aboelfotoh and Noha A Hikal. "A review of cyber-security measuring and assessment methods for modern enterprises." In: *JOIV: International Journal on Informatics Visualization* 3.2 (2019), pp. 157–176.

[Fit19] Laura Fitzgibbons. *states of digital data*. https://searchdatamanagement.techtarget.com/reference/states-of-digital-data. [Accessed: 2022-02-09]. Feb. 2019.

[GM19] Hamidreza Ghorbani and M Saeed Mohammadzadeh. "Review on iot standards and suggesting a new method to enhance data security." In: *2019 Third International conference on ISMAC (IoT in Social, Mobile, Analytics and Cloud)(ISMAC)*. IEEE. 2019, pp. 152–158.

[El-+19] Mohammed El-Hajj et al. "A survey of internet of things (IoT) authentication schemes." In: *Sensors* 19.5 (2019), p. 1141.

[Has+19] Wan Haslina Hassan et al. "Current research on Internet of Things (IoT) security: A survey." In: *Computer networks* 148 (2019), pp. 283–294.

[Kha+19] Manju Khari et al. "Securing data in Internet of Things (IoT) using cryptography and steganography techniques." In: *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50.1 (2019), pp. 73–80.

[LČH19] Björn Leander, Aida Čaušević, and Hans Hansson. "Applicability of the IEC 62443 standard in Industry 4.0/IIoT." In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. 2019, pp. 1–8.

[Sko19] Christina Skouloudi. *Good practices for security of IoT*. Nov. 2019. URL: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1.

[Vin+19] Ravi Vinayakumar et al. "Deep learning approach for intelligent intrusion detection system." In: *IEEE Access* 7 (2019), pp. 41525–41550.

[Ali+20] Aliyu Aliyu et al. "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom." In: *Applied Sciences* 10.10 (2020), p. 3660.

[Alm+20] Muder Almiani et al. "Deep recurrent neural network for IoT intrusion detection system." In: *Simulation Modelling Practice and Theory* 101 (2020), p. 102031.

[AS20] Ömer Aslan Aslan and Refik Samet. "A comprehensive review on malware detection approaches." In: *IEEE Access* 8 (2020), pp. 6249–6271.

[BFL20] Gioele Bigini, Valerio Freschi, and Emanuele Lattanzi. "A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision." In: *Future Internet* 12.12 (2020), p. 208.

[BJH20] Paul Brous, Marijn Janssen, and Paulien Herder. "The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations." In: *International Journal of Information Management* 51 (2020), p. 101952.

[Con20] H.R.1668 116th Congress. *IoT Cybersecurity Improvement Act of 2020*. https://www.congress.gov/bill/116th-congress/house-bill/1668. [Accessed: 2022-01-24]. Dec. 2020.

[Gan+20] Alexander A Ganin et al. "Multicriteria decision framework for cybersecurity risk assessment and management." In: *Risk Analysis* 40.1 (2020), pp. 183–199.

[IEC20] IEC. *Quick start guide: An overview of isa/iec 62443 standards, isa global cybersecurity alliance*. June 2020. URL: https://cdn2.hubspot.net/hubfs/5382318/ISAGCA%5C%20Quick%5C%20Start%5C%20Guide%5C%20FINAL.pdf.

[Kan+20] Kamalanathan Kandasamy et al. "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process." In: *EURASIP Journal on Information Security* 2020.1 (2020), pp. 1–18.

[KSH20] Nickson M Karie, Nor Masri Sahri, and Paul Haskell-Dowland. "IoT threat detection advances, challenges and future directions." In: *2020 workshop on emerging technologies for security in IoT (ETSecIoT)*. IEEE. 2020, pp. 22–29.

[KL20] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. CRC press, 2020.

[Ora20] Oracle. *What is IoT?* https://www.oracle.com/nl/internet-of-things/what-is-iot/. [Accessed: 2022-02-01]. 2020.

[Sha+20] Kamran Shaukat et al. "Cyber threat detection using machine learning techniques: A performance evaluation perspective." In: *2020 International Conference on Cyber Warfare and Security (ICCWS)*. IEEE. 2020, pp. 1–6.

[Sko+20] Christina Skouloudi et al. *ENISA Report - Guidelines for Securing the Internet of Things*. Nov. 2020. URL: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things.

[SBW+20] S Smys, Abul Basar, Haoxiang Wang, et al. "Hybrid intrusion detection system for internet of things (IoT)." In: *Journal of ISMAC* 2.04 (2020), pp. 190–199.

[SSJ20] Dhanda Sumit, Brahmjit Singh, and Poonam Jindal. "Lightweight Cryptography: A Solution to Secure IoT." In: *Wireless Personal Communications* 112 (June 2020), pp. 1–34. DOI: 10.1007/s11277-020-07134-3.

[Ahm+21] Zeeshan Ahmad et al. "Network intrusion detection system: A systematic study of machine learning and deep learning approaches." In: *Transactions on Emerging Telecommunications Technologies* 32.1 (2021), e4150.

[BR+21] Shobha Bhatt, Prakash Rao Ragiri, et al. "Security trends in Internet of Things: A survey." In: *SN Applied Sciences* 3.1 (2021), pp. 1–14.

[Bla21] Borka Jerman Blažič. "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?" In: *Education and Information Technologies* (2021), pp. 1–26.

[Cha+21] Jeffrey S Chavis et al. "TOWARD ASSURANCE AND TRUST FOR THE INTERNET OF THINGS." PhD thesis. Johns Hopkins University, 2021.

[DB21] Suparna Dhar and Indranil Bose. "Securing IoT devices using zero trust and blockchain." In: *Journal of Organizational Computing and Electronic Commerce* 31.1 (2021), pp. 18–34.

[DG21] Sachin Dhawan and Rashmi Gupta. "Analysis of various data security techniques of steganography: A survey." In: *Information Security Journal: A Global Perspective* 30.2 (2021), pp. 63–87.

[Ech+21] Aarón Echeverría et al. "Cybersecurity model based on hardening for secure internet of things implementation." In: *Applied Sciences* 11.7 (2021), p. 3260.

[Gao+21] Runchen Gao et al. "A lightweight cryptographic algorithm for the transmission of images from road environments in self-driving." In: *Cybersecurity* 4.1 (2021), pp. 1–11.

[Iwa21] Takehisa Iwakoshi. "Security Evaluation of Y00 Protocol Based on Time-Translational Symmetry Under Quantum Collective Known-Plaintext Attacks." In: *IEEE Access* 9 (2021), pp. 31608–31617.

[Jov21] Bojan Jovanović. *Internet of Things statistics for 2021 - Taking Things Apart*. Ed. by DataProt. [Online; posted 24-March-2021]. Mar. 2021. URL: https://dataprot.net/statistics/iot-statistics/.

[Kar+21] Nickson M. Karie et al. "A Review of Security Standards and Frameworks for IoT-Based Smart Environments." In: *IEEE Access* 9 (2021), pp. 121975–121995. DOI: 10.1109/ACCESS.2021.3109886.

[LK21] Manju Lata and Vikas Kumar. "Standards and Regulatory Compliances for IoT Security." In: *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET)* 12.5 (2021), pp. 133–147.

[Lee21] In Lee. "Cybersecurity: Risk management framework and investment cost analysis." In: *Business Horizons* 64.5 (2021), pp. 659–671.

[Lel21] Ifigeneia Lella. *ENISA Threat LANDSCAPE 2021*. 2021.

[Les21] RafaÅ Leszczyna. "Review of cybersecurity assessment methods: Applicability perspective." In: *Computers Security* 108 (2021), p. 102376. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2021.102376. URL: https://www.sciencedirect.com/science/article/pii/S0167404821002005.

[Lia+21] Zitian Liao et al. "Assessing security of software components for Internet of Things: a systematic review and future directions." In: *Security and Communication Networks* 2021 (2021).

[MSB21] Yassine Maleh, Abdelkebir Sahid, and Mustapha Belaissaoui. "A maturity framework for cybersecurity governance in organizations." In: *EDPACS* 63.6 (2021), pp. 1–22.

[OLS21] Bilge Yigit Ozkan, Sonny van Lingen, and Marco Spruit. "The Cybersecurity Focus Area Maturity (CYSFAM) Model." In: *Journal of Cybersecurity and Privacy* 1.1 (2021), pp. 119–139.

[PwC21] PwC. *Protecting the connected world: IoT security at a turning point*. https://www.pwc.com/us/en/tech-effect/cybersecurity/iot-security.html. [Accessed: 2022-01-24]. Mar. 2021.

[Qiu+21] Song Qiu et al. "Performance analysis of a fail-safe wireless communication architecture for IoT based fire alarm control panels." In: *SN Applied Sciences* 3.3 (2021), pp. 1–8.

[RDC21] A Reeves, P Delfabbro, and D Calic. "Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue." eng. In: *SAGE open* 11.1 (2021), p. 215824402110000. ISSN: 2158-2440.

[TRK21] Vishal A Thakor, Mohammad Abdur Razzaque, and Muhammad RA Khandaker. "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities." In: *IEEE Access* 9 (2021), pp. 28177–28193.

[WG121] IoT SF WG1. *IoTSF IoT Security Assurance Framework Release 3.0 Nov 2021*. Nov. 2021. URL: https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf.

[IBM22] IBM. *What is cybersecurity?* https://www.ibm.com/topics/cybersecurity. [Accessed: 2022-02-03]. 2022.

[KS22] Olena Klisenko and Estefanía Serral Asensio. "Towards a Maturity Model for IoT Adoption by B2C Companies." In: *Applied Sciences* 12.3 (2022), p. 982.

[PwC22] PwC. *OT IoT Security*. https://www.pwc.de/de/im-fokus/cyber-security/ot-und-iot-security.html. [Accessed: 2022-02-23]. Jan. 2022.

[IEC22] IEC. *Information security, cybersecurity and privacy protection*. Standard. Geneva, CH: International Organization for Standardization, Feb. 2022.

Chapter 8

Appendix

8.1 Appendix A: Semi-structured interview guide

1. Introduction to the research and structure of the interview

    - Discuss the scope of this research
    - Personal information
    - Personal experience/insights on the topic
    - Verify the up to now collected insights on IoT challenges and available assessment methods
    - What can be implemented? And what should that look like?

2. Explain the words below.

    - Explain the purpose of the recording
    - Explain why the recording will be maintained and for how long
    - Interviewee has the right to stop the interview at any time and request the interview to be deleted
    - Afterwards the interview will be transcribed and anonymized. (whenever interested the interviewee has the right to read the transcription, to minimize confidential data)
    - Do you give me the consent to record the interview?

3. What is your field of expertise? What is your background (education and work)? How many years of experience in this field do you have?

4. What is your current role? And what does it involve in terms of activities and responsibilities?

5. In what country do you work? In what ways would this differ from other countries, e.g. specialized offices, clients?

6. From your point of view, how would you describe IoT?

7. Do you have any experience with assessments on IoT-based environments? If not, what comes the closest?

    - Were you encountering problems / gaps in the process? What made it special?
    - What could be possible improvements?

8. Verify SQ1: Discuss current limitations in assessment frameworks

    - What is essential in a comprehensive assessment framework? (Discuss the proposed fishbone diagram in figure 2.5 and the list in Appendix B)
    - What are essential outcomes in comprehensive assessment frameworks? (current risks, feedback, educational needs, managerial improvements, detection methods, and available software)
    - What are the main challenges in IoT? (technical, legal, ethical, operational, and adaptive)
    - What are the issues in making a framework applicable?

9. Verify SQ2: Discuss how risks can be assessed

    - **To assess the own created framework:**
    - How can we assess the comprehensiveness of the framework?
    - How can we assess the comprehensiveness of the outcomes?
    - **Assess the challenges in networks:**
    - How can we assess the applicable challenges? (8 framework points)
    - How can we assess the technical challenges? (NIST, economical, threats, vulnerabilities, and consequences)
    - How can we assess the legal challenges? (legislative monitoring)
    - How can we assess the ethical challenges? (POLP)

- How can we assess the operational challenges? (standardization, assessment repeat, and internal knowledge)
- How can we assess the adaptive challenges? (structure management, implemented monitoring)

10. Verify SQ3: Discuss solutions to IoT challenges
    - Where must be focused on to provide safe IoT? (11 future solutions, **securing different layers**)
    - What are the latest and most relevant technological improvements? (encryption, authentication, blockchain, IDS)
11. Ask about SQ4: What overall process or guidelines can be implemented to improve the security of IoT-based environments? (Should this be NIST or better alternative?)
12. Ask about SQ5: How can the IoT-based environment security be generalized into an overall applicable assessment framework? (How to add upon NIST?)
13. Are there any other topics you find relevant to discuss or mention in this field?
14. Discussion to improve the current framework that is in progress. How and what should be changed?
15. Are you available for follow-up questions?
16. Are you interested in receiving the final transcriptions?

8.2 Appendix B: List for comprehensive framework

- Environment assessment
- Risk assessment
- Security standards
- Management assessment
- Regulations monitoring
- Maturity assessment

8.3 Appendix C: Coding (sub-)categories concepts

Category	**Sub-category**	**Concept**
Existing frameworks	Risk framework	COSO ERM
Existing frameworks	Risk framework	CIA
Existing frameworks	Risk framework	IRAM2
Existing frameworks	Cybersecurity framework	ENISA
Existing frameworks	Cybersecurity framework	NIST
Existing frameworks	Cybersecurity framework	IEEE
Existing frameworks	Cybersecurity framework	IOTSF
Existing frameworks	Cybersecurity standards	ISO
Existing frameworks	Cybersecurity standards	IEC
Existing frameworks	Cybersecurity standards	NERC-CIP
Existing frameworks	Cybersecurity standards	ISF
IoT	IoT types	Consumer IoT
IoT	IoT types	Industrial IoT
IoT	IoT types	Operational Technology (OT)
IoT challenges	Technical development	Outdated devices
IoT challenges	Technical development	Outdated software
IoT challenges	Technical development	Not supported devices
IoT challenges	Technical development	Do not meet security standard
IoT challenges	Technical development	Attack vector
IoT challenges	IT-OT-IoT convergence	One security framework
IoT challenges	IT-OT-IoT convergence	Different standards
IoT challenges	IT-OT-IoT convergence	Different expertise
IoT challenges	IT-OT-IoT convergence	Limited security capabilities
IoT challenges	Lack in regulation	Lack in standards
IoT challenges	Lack in regulation	Lack in vendor regulation
IoT challenges	Lack in regulation	Device analysis
IoT challenges	Lack in regulation	Conflicting priorities
IoT challenges	Lack in regulation	Maintenance service contracts
IoT challenges	Size of the environment	Amount of devices
IoT challenges	Size of the environment	Scalability of the attack
IoT challenges	Size of the environment	Combination of data
IoT challenges	Size of the environment	Attacking surface
IoT challenges	Size of the environment	Weakest link
IoT challenges	Limited expertise	Human problem
IoT challenges	Limited expertise	Low internal expertise

IoT challenges	Limited expertise	Based on own experience
IoT challenges	Device related services	Function instead of security
IoT challenges	Device related services	Limited possibilities
IoT challenges	Operational	Continuous innovation
IoT challenges	Operational	Learn-unlearn-learn cycle
IoT challenges	Operational	Physical devices
IoT challenges	Operational	Processes and standards
IoT challenges	Interoperability	Dependent on other devices
IoT challenges	Interoperability	Chain of trust
IoT challenges	Interoperability	Reliability
IoT challenges	Adaptability	Not willing to change
IoT challenges	Adaptability	Priority contrasts
IoT challenges	Adaptability	Trust limitations
IoT challenges	Connectivity	Implicates risk
IoT challenges	Connectivity	Retrieve data from air
IoT challenges	Diversity	Diversity in devices
IoT challenges	Diversity	Diversity in network
IoT challenges	Data	Data storage
IoT challenges	Data	Data processing
IoT challenges	Data	Data at rest
IoT challenges	Data	Data in motion
IoT challenges	Data	Data at use
IoT challenges	Data	Availability
Framework limitations	No existing framework	Immature frameworks
Framework limitations	No existing framework	Incomplete frameworks
Framework limitations	No existing framework	Specialized frameworks
Framework limitations	No existing framework	Outdated frameworks
Framework limitations	No one size fits all	Different security levels
Framework limitations	No one size fits all	Combining frameworks
Framework limitations	No one size fits all	Domain specific frameworks
Framework limitations	Created by the industy	Not highest requirements
Framework limitations	Assess static network	Network changes quickly
Framework limitations	Applicability	Generic/specific-trade-off
Framework limitations	Applicability	High level guidance
Framework limitations	Applicability	Domain specific
Framework guidelines	Sections	General outline
Framework guidelines	Sections	Controls
Framework guidelines	Sections	Assessment

Framework guidelines	Assessment	Rule based philosophy
Framework guidelines	Assessment	Principle based philosophy
Framework guidelines	Assessment	Technical assessment
Framework guidelines	Assessment	Comprehensive
Framework challenges	Scope	Holistic network
Framework challenges	Scope	IT-OT-IoT convergence
Framework challenges	Combine frameworks	Not build to fit
Framework challenges	Combine frameworks	Used to these frameworks
Framework challenges	Combine frameworks	NIST
Framework challenges	Combine frameworks	ENISA
Framework challenges	Combine frameworks	IEC
Framework challenges	Security by design	Secure before implementation
Framework challenges	Security by design	Monitor devices
Framework challenges	Security by design	Costly to erase devices
Framework challenges	Security by design	Engineer not cyber prof
Framework challenges	Objective assessment	Self-assessment
Framework challenges	Objective assessment	Descriptive facts
Framework challenges	Objective assessment	Necessary expertise
Framework challenges	Flexible framework	Applicable
Framework challenges	Flexible framework	Dynamic
Framework challenges	Flexible framework	Periodic loop
Comprehensive framework	Generic/specific tradeoff	Generic part applies always
Comprehensive framework	Generic/specific tradeoff	More specific sections
Comprehensive framework	Generic/specific tradeoff	If-clause
Comprehensive framework	Generic/specific tradeoff	In-depth technical framework
Comprehensive framework	Framework testing	Simply cover everything
Comprehensive framework	Framework testing	Low hanging fruit
Comprehensive framework	Framework testing	Semi automated manner
Comprehensive framework	Framework testing	Cluster attributes
Comprehensive framework	Framework testing	Match attack to cluster
Comprehensive framework	Framework testing	Generate all possible threats
Comprehensive framework	Framework outcome	To do list
Comprehensive framework	Framework outcome	Transformation roadmap
Comprehensive framework	Framework outcome	Guidance
Comprehensive framework	Framework outcome	Prioritization of issues
Comprehensive framework	Framework outcome	Feedback
Comprehensive framework	Framework outcome	Descriptive facts
Comprehensive framework	Framework outcome	Action driven feedback

Comprehensive framework	Framework outcome	CVE
Comprehensive framework	Framework outcome	Process/validate/remediate
Comprehensive framework	Framework outcome	3 pillars of transformation
Comprehensive framework	Risk assessment	Always some risk
Comprehensive framework	Risk assessment	Risk awareness
Comprehensive framework	Risk assessment	Risk identification
Comprehensive framework	Risk assessment	Financial risk
Comprehensive framework	Risk assessment	People risk
Comprehensive framework	Risk assessment	Reputation risk
Comprehensive framework	Risk assessment	Technological risk
Comprehensive framework	Risk assessment	Compliance/regulatory-risks
Comprehensive framework	Risk assessment	Product failure
Comprehensive framework	Risk assessment	Threat modeling
Comprehensive framework	Risk assessment	Vulnerability
Comprehensive framework	Risk assessment	Consequences
Comprehensive framework	Risk assessment	Likelihood
Comprehensive framework	Management assessment	Management requirements
Comprehensive framework	Management assessment	Conflicting priorities
Comprehensive framework	Management assessment	Cost-benefit-analysis
Comprehensive framework	Management assessment	Security as limitation
Comprehensive framework	Management assessment	User training
Comprehensive framework	Management assessment	User awareness
Comprehensive framework	Management assessment	Old devices limitations
Comprehensive framework	Management assessment	Old protocols limitations
Comprehensive framework	Management assessment	Miscommunication
Comprehensive framework	Management assessment	Access management
Comprehensive framework	Management assessment	Change management
Comprehensive framework	Management assessment	Zero day attack
Comprehensive framework	Management assessment	Thinking ahead
Comprehensive framework	Management assessment	Monitoring
Comprehensive framework	Management assessment	Key risk indicators (KRI)
Comprehensive framework	Management assessment	KPI
Comprehensive framework	Management assessment	Pen testing
Comprehensive framework	Management assessment	Vulnerability management
Comprehensive framework	Management assessment	Asset management
Comprehensive framework	Management assessment	People assessment
Comprehensive framework	Management assessment	Connect monitor to solution
Comprehensive framework	Maturity assessment	Corbit maturity framework

Comprehensive framework	Maturity assessment	Capability maturity model
Comprehensive framework	Maturity assessment	Maturity level
Comprehensive framework	Maturity assessment	Security level
Comprehensive framework	Maturity assessment	Minimize data collection
Comprehensive framework	Maturity assessment	Organizational maturity
Comprehensive framework	Maturity assessment	Understand the technology
Comprehensive framework	Maturity assessment	Involved security experts
Comprehensive framework	Maturity assessment	Department dependencies
Comprehensive framework	Security standards	All level mitigations
Comprehensive framework	Security standards	Secure architecture
Comprehensive framework	Security standards	Secure access control
Comprehensive framework	Security standards	Secure data traffic
Comprehensive framework	Security standards	Secure protocols
Comprehensive framework	Security standards	Secure software development
Comprehensive framework	Regulation monitoring	Regulatory stakeholder cycle
Comprehensive framework	Regulation monitoring	Case specific
Comprehensive framework	Regulation monitoring	Contract monitoring
Comprehensive framework	Regulation monitoring	Manufacturing contract
Comprehensive framework	Regulation monitoring	Maintenance contract
Comprehensive framework	Regulation monitoring	Maintenance service
Comprehensive framework	Regulation monitoring	GDPR
Comprehensive framework	Regulation monitoring	PIPEDA
Comprehensive framework	Regulation monitoring	NGO-regulations
Comprehensive framework	Regulation monitoring	Network specific laws
Comprehensive framework	Regulation monitoring	Sanction monitoring
Comprehensive framework	Regulation monitoring	Vague described concepts
Comprehensive framework	Regulation monitoring	Privacy
Comprehensive framework	Regulation monitoring	Compliance
Comprehensive framework	Regulation challenges	Regulating design
Comprehensive framework	Regulation challenges	Conflicting interests
Comprehensive framework	Regulation challenges	Responsibility
Comprehensive framework	Regulation challenges	Outdated regulations
Comprehensive framework	Regulation challenges	Grey area
Comprehensive framework	Regulation challenges	User protection
Comprehensive framework	Regulation challenges	User awareness
Comprehensive framework	Regulation challenges	Manufacturer cycle
Comprehensive framework	Environment assessment	Scope of risk
Comprehensive framework	Environment assessment	Scalability of the attack

Comprehensive framework	Environment assessment	Asset identification
Comprehensive framework	Environment assessment	Criticality of the asset
IoT security solutions	Limited protocols	Standardization
IoT security solutions	Limited protocols	Enforce minimal security
IoT security solutions	Limited protocols	Minimal basic config
IoT security solutions	Limited protocols	foundational controls
IoT security solutions	Limit attack scalability	Segmentation
IoT security solutions	Secure data traffic	5G
IoT security solutions	Limit data traffic	Internal processing
IoT security solutions	Secure architecture	Zero trust architecture
IoT security solutions	Secure architecture	Basic cyber hygiene
IoT security solutions	Secure architecture	Product life cycle
IoT security solutions	Secure architecture	Trusted platform module
IoT security solutions	Secure authentication	Lightweight algorithms
IoT security solutions	Awareness	User training
IoT security solutions	Encryption	End-to-end connectivity
IoT security solutions	Encryption	Lightweight algorithms
IoT security solutions	Critical risks	Analog layer
IoT security solutions	Privacy	Principle of least priveliged
IoT security solutions	Vendor responsibilities	Enforce security updates
IoT security solutions	Vendor responsibilities	Security by design
IoT security solutions	Vendor responsibilities	Default secure architecture
IoT security solutions	Security enforcement	Regulations
IoT security solutions	Secondary security	Firewall
IoT security solutions	Secondary security	Cloud solutions
IoT security solutions	Secondary security	Patching
IoT security solutions	Secondary security	Access control list
IoT security solutions	Secondary security	Threat landscapes
IoT security solutions	Secondary security	Unique factorization domain
IoT security solutions	Secondary security	Fail safe system
IoT security solutions	Secondary security	Boundary defense
IoT security solutions	Security software	NOZOMI
IoT security solutions	Security software	Defender for IoT
IoT security solutions	Security software	Dragos
IoT security solutions	Security software	RMIS
Framework guidelines	Scope	Distinguish public/private
Framework guidelines	Scope	Distinguish OT/IoT
Framework guidelines	Scope	Industrial IoT

Framework guidelines	Scope	Mainstream IoT
Framework guidelines	Framework type	Dynamic framework
Framework guidelines	Framework type	Build on best existing
Framework guidelines	Existing frameworks	Already in use
Framework guidelines	Existing frameworks	Argue the importance
Framework guidelines	Existing frameworks	Reusing
Framework guidelines	Create value	Make it worth to use new
Framework guidelines	New framework	Be innovative
Framework guidelines	New framework	Create own vision
Framework guidelines	Validate	Build upon framework
Framework guidelines	Validate	Rely on research
Framework guidelines	Validate	Four eyes principle
Framework guidelines	Validate	Check with experts