MASTER THESIS

MANAGING CYBER RISKS IN SMART CITIES

Name: M.A.J. (Mathijs) Pondes

Faculty: Behavioural, Management and Social Sciences

Master: Business Administration

Track: Digital Business

1st supervisor: dr. A. Abhishta

2nd supervisor: dr. M. de Visser

External Supervisor: W. Uijlenberg

24-8-2020

Acknowledgements

During the specialization track Digital Business of the master Business Administration at the University of Twente, I had the chance to discover more about the role of IT within organizations. New technologies, like the Internet of Things, were discussed and aroused my interest. I applied at BDO Audit & Assurance B.V. in Hengelo to write my thesis about it. Fortunately, the organization is specialized in auditing and advising municipalities, and gave me the chance to perform a research about the cyber risks for smart cities. I would like to thank Ward Uijlenberg, who provided me the necessary expertise about the topic. Furthermore, I appreciated that Ward and his colleagues were open for questions throughout the whole process of this thesis, even though we had to communicate from home, due to the COVID-19 outbreak. Besides, I would like to thank my supervisors dr. Abhishta and dr. de Visser of the University of Twente, for sharing their feedback, opinions and new insights that I could implement during the thesis. Lastly, I would like to acknowledge the organizations who provided the practical risks and countermeasures that were applied in this thesis.

Hopefully you will enjoy reading this thesis, and be able to retrieve new insights from the content. If any questions arise, feel free to contact me.

Kind regards,

Mathijs Pondes

‘s-Hertogenbosch, 24-08-2020

Abstract

The world's urban population is growing, creating better living standards for citizen. Yet, this also comes forth with new challenges, like traffic congestion and pollution. Smart cities are introduced as a solution to these problems, using advanced ICT technologies to create a sustainable, efficient and innovative urban environment to improve the quality of life of its citizens. In smart cities, a high number of interconnected and intelligent devices are placed in the city's infrastructure, enabling digital solutions for current physical operations. Smart cities have numerous advantages, but they also bring new cybersecurity challenges that need to be managed. This can be hard, as standards on securing smart cities are currently missing. Furthermore, scientific literature does not cover a comprehensive management framework on the risks, making it hard to understand which parts of cybersecurity are typically important for smart cities. In this thesis, the cyber risks and several countermeasures are combined into a risk management framework, to tackle these issues.

The research is set up as follows. First, an exploratory literature review is carried out to get an understanding of the concept of smart cities, cybersecurity and risk management. Then, a systematic literature is completed, by analyzing 108 papers and using 22 papers to find the typical cyber risks for smart cities. Followed by five interviews with representatives from smart cities, to combine theory with experiences from practice. The risks are analyzed and prioritized based on their relevance to the smart city characteristics. Furthermore, experts from BDO were asked about what they see as the most important factors for a framework for smart cities. Next, countermeasures were drawn up, based on requirements for current smart city public procurements, prior research within this thesis (like the interviews and SLR), and literature. The risks and countermeasures are linked based on the cybersecurity category they apply to. In the end, a framework is proposed that combines the research on the topics of smart cities, cybersecurity and risk management.

The main contribution of the proposed framework is that it can be used to advise information security experts from smart cities on how to manage cyber risks. The cyclic risk management process that could be followed is depicted (Figure 13), giving the process steps that smart city executives should take. In doing so, they are assisted by the proposed risks and countermeasures of this thesis. In total, 30 risks are identified, of which 23 were seen as typical smart city risks that are taken into further analysis. Depending on the internal and external context of the organization, the practical outcome of the risk management framework will differ per smart city.

Contents

1. Introduction

1.1 Introduction

The urban population is expected to grow from 55% to 68% of the total world population in 2050 (UN, 2018). Urbanisation has improved the world's living standards for citizens, for example by improved services like healthcare and education, as well as the living and working environment (Xie et al., 2019). On the other hand, Xie et al. (2019) state that it also includes new challenges, like traffic congestion, waste, air and gas pollution. Smart city is introduced as a solution to these problems, focusing on improved quality of life of a municipality's citizens and creating a sustainable urban environment by applying advanced Information and Communication Technology (ICT) (Xie et al., 2019). These advanced technologies can be described by the devices that the city and its citizens are instrumented with, which are interconnected and intelligent (Elmagrabhy & Losavio, 2014). In other words, these devices are able to communicate information through a network, in order to do analysis and decision-making. Putting all these devices together within the smart city forms its internet of things (IoT) (Gharaibeh et al., 2017). The research and advisory company Gartner (2018) forecasts that 25 billion IoT devices are present in 2021, creating loads of data. And many of these devices are part of the municipal infrastructure, ranging from end-user devices to municipal systems (Gharaibeh et al., 2017).

Yet, the cybersecurity of these systems appears to be vulnerable and smart cities face new challenges compared to 'usual' cities. First, because these devices are connected, the attack surface increases (Kahn & Salah, 2018). Recent entries by cyber criminals in the cloud computing systems of private and public organizations in The Netherlands shows the relevance of the topic (NOS, 2020). Second, because of the large number of devices in public space, which are tangible by others. Furthermore, many different devices lead lots of different involved suppliers and technologies as well. Third, smart cities process sensitive data, which could lead to privacy breaches of the citizens if not processed correctly. Fourth, smart cities are able to put a connection between the digital and the physical world. This shows the importance of cybersecurity in smart cities, since this also contains the critical infrastructure of municipalities. If a service goes down, this could have a great impact on the municipality.

This implies that cybersecurity is an important factor for smart cities. However, the internet of things is developing rapidly and developers have to meet deadlines in order to be competitive (Habibzadeh et al., 2019). According to Habibzadeh et al. (2019), this results in immature products containing which is seen as a feature, and added in a later stage. The current COVID-19 outbreak showed the same trends. For example, the outbreak resulted in a high demand for systems that can track people who might be infected by the virus (NOS, 2020a). Applications like the COVID-19 app are typical for smart cities. The devices communicate via a Bluetooth network, and the user can decide to change his plans if he had been close to an infected person. But when they were tested possible apps in The Netherlands halfway April 2020, it appeared that all of the suppliers had issues to enhance the security requirements in their offered apps (Rijksoverheid, 2020).This pictures the problem for smart cities quite well, as suppliers try to quickly and efficiently create smart city products, at the expense of cybersecurity.

Therefore, municipalities should know how to manage the cyber risks that come forth by implementing smart city applications. The goal of this research is to propose a cyber risk management framework for smart cities. A risk management framework gives the organizational risk and the way to manage these risks (NIST, 2020). Which is required, as enabling technologies like IoT are adopted in smart cities, but current cybersecurity standards hardly take the forthcoming cyber risks into account. Furthermore, current scientific literature does not look at the cyber risks for smart cities from a management perspective, explaining the contribution of this thesis to current scientific research.

The framework is compiled to advise information security officers of smart cities in how to perform cyber risk management in smart cities, by giving the typical risks and countermeasures. Based on the risks from theory and practice, information security officers can check the applicability to their smart city, which is usually done in collaboration with colleagues from different departments. Once only the relevant risks remain, smart cities could choose to treat these risks in four different ways, namely by reducing, avoiding, transferring or accepting the risks. If information security officers decide to reduce the risk by improving the information security level, this thesis can contribute by providing several countermeasures in order to find appropriate treatments. Internally and externally communicating about the risk management practices could be valuable for a smart city, as it could increase citizen acceptance, which is one of the success factors of smart cities (Lim, Edelenbos, & Gianoli, 2019).

This paper is structured as follows. Chapter 2 gives an exploratory literature review on smart cities, information security and its threats, followed by the methodology in chapter 3. Chapter 4 contains the results, including the cyber risks and controls based on theoretical and practical findings. The last chapter provides the discussion and conclusion.

1.2 Profile of the company

The research is carried out at *BDO Audit & Assurance B.V. (BDO)*, located in Hengelo, The Netherlands. A large part of the clients of BDO consists of public organizations. The organization provides audit, risk and assurance services for their clients, also regarding cybersecurity. Due to the rise of the IoT, municipalities are starting to implement ‘smart’ solutions. However, the current cybersecurity standard in The Netherlands for governmental institutions, the Baseline Informatiebeveiliging Overheid (BIO), takes the cybersecurity risks of IoT hardly into account. The BIO focuses on confidentiality, whereas availability and integrity of information are especially important for IoT implementations. The framework proposed in this paper could therefore be valuable for BDO, in order to advise their clients on the cybersecurity risks for smart cities and how to manage them.

Besides, the author of this thesis also takes advantage of this collaboration as well. Being able to ask questions throughout the whole process, made it easier to understand industry specific concepts and context information on cybersecurity of governmental institutions. Furthermore, the knowledge of experts of BDO is used in the validation study of this thesis.

1.3 Research questions

In order to stay attractive to (potential) citizens, a city should take care of an innovative and sustainable environment. Implementing smart city projects is one of the ways to do this, yet it comes with new cyber risks. These are quite unknown and often not yet taken into account in current cybersecurity management standards, like the BIO (2020) in The Netherlands. Therefore, the goal of this paper is to propose a cyber risk management framework for smart cities. And the following main research question is proposed:

RQ: “How can smart cities manage their cyber security risks?”

In order to answer this question, five sub-questions need to be answered as well (Table 1). The questions are summed and explained in the following paragraphs.

SQ1: “What are smart cities, cybersecurity, and risk management?”

Sub-question 1 is proposed to get an understanding of the three concepts smart city, cybersecurity and risk management. Scientific literature is used to get an understanding of the concepts. In order to understand cyber security and risk management, standards for practice are used as well. This sub-question results in smart city characteristics, which will be used to prioritize the cyber risks. Furthermore, it gives a broad overview of the cybersecurity categories. These categories are used to divide the risks accordingly. The concept of risk management is included to get an understanding of risk management processes. The information is used to put the risks and countermeasures together in a framework.

SQ2: “What are the cyber risks associated with smart cities?”

The second sub-question is proposed to get an understanding of the cyber risks in smart cities. This question is answered from a practical and scientific perspective, to get a broad view on the topic and find risk factors that are not discussed in theory. Scientific findings come forth from a systematic literature review as described by Webster and Watson (2002). The practical findings are derived from five different interviews, which represent three municipalities, one energy net provider and three regional water authorities.

SQ3: "Which factors as discussed in sq2 should be taken into account in a cyber risks management framework for smart cities?"

To make sure that the risks are typical risks for smart cities, they are filtered by the characteristics of smart cities. The characteristics as described in sq1 are used to filter the risks as described in sq2.

SQ4: "What are the countermeasures regarding the cyber risks?"

Currently, research on the countermeasures already exists, however, not yet from the point of cyber risk management. This thesis aims to find the countermeasures that belong to the cyber risks as proposed in SQ2 and categorizes them based on the cybersecurity categories that are drawn up in SQ1. There are three different sources used to answer SQ3. The earlier described interviews and papers from the systematic literature review are used. Furthermore, this thesis uses security requirements of public tenders that are drawn up for purchasing IoT devices.

SQ5: "Which factors can be added, changed or removed, in order to improve the framework?"

This question is proposed to validate the research. Experts of BDO are asked to participate in a validation study, which is presented as an interview. Based on a newspaper article, the interviewees can elaborate on how the framework could contribute to future smart cities' directors on what is implied regarding cybersecurity. Furthermore, they will be asked how the framework could be further improved.

Sub-question	Purpose	Methodology	Ch.
1. What are smart cities, cybersecurity and risk management?	Understanding of the concept	Exploratory literature review	2
2. What are the cyber risks associated with smart cities?	Overview of the cyber risks & Prioritization (if in line with sc characteristics)	Exploratory literature review Systematic literature review Interviews (smart cities)	4
3. Which factors as discussed in sq2 should be taken into account in a cyber risks management framework for smart cities?	Draw up the cyber risk management framework	Reuse information	2 & 4
4. What are the countermeasures regarding the cyber risks?	Overview of related countermeasures	Review of standards Exploratory literature research	4
5. Which factors can be added, changed or removed, in order to improve the framework?	Validation of the framework	Interviews (experts BDO)	4

Table 1 Research questions and methodologies

1.4 Structure

This section provides an overview of the research structure, to get an understanding of how the research questions are investigated in practice (Figure 1). Chapter 2 gives a background by describing smart cities, information security and risk management, which is step 1 of the structure. Chapter 3 gives an explanation on the methodology of this thesis. Chapter 4 contains the results on the retrieved risks and countermeasures. This includes research step 2, 3, 4 and 5. Chapter 5 provides a conclusion and discussion.

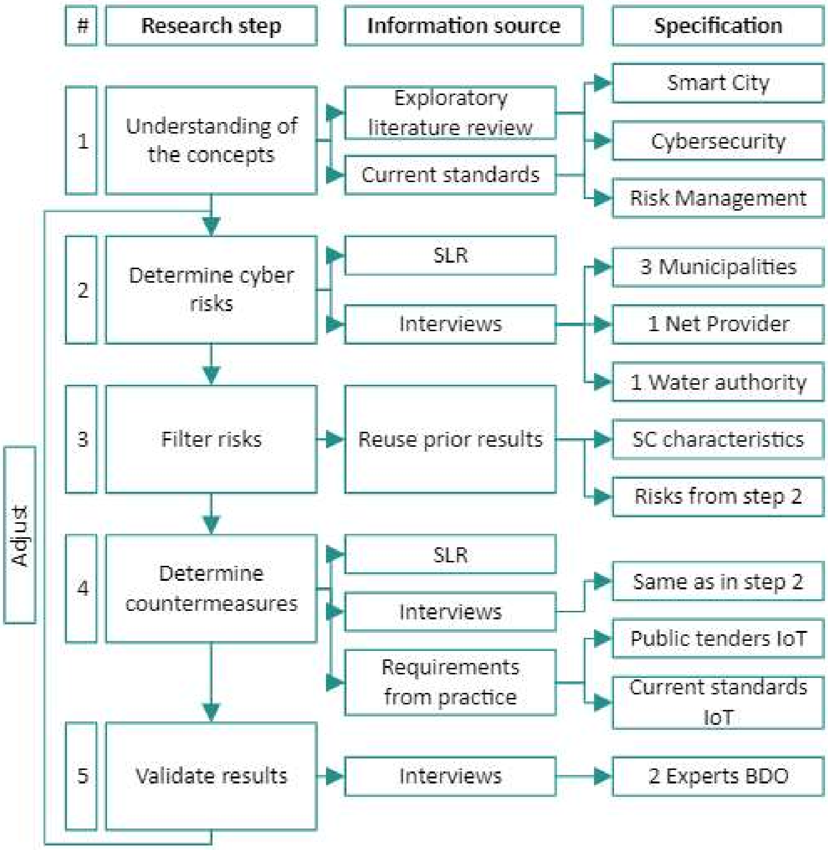


Figure 1 Research structure

2. Theoretical framework

This section describes the key papers and concepts of this research. The following topics are discussed: smart cities, cyber security and risk management. The exploratory research on theory, using literature reviews on smart cities as a starting point (Albino, Berardi, & Dangelico, 2015; Ismagilova, Hughes, Dwivedi, & Raman, 2019). Besides, current cybersecurity management frameworks are used in this chapter to get an understanding of cybersecurity (BIO, 2020; ISF, 2020, NIST, 2018, NCSC, 2019). Lastly, the widely accepted COSO (2015) is used give an explanation on the basics of risks management.

2.1 Smart cities

The concept of smart city exists for more than twenty years, and its definition has changed during that period. At first, it was conceptualized from a technical perspective in the 1990s, explaining its contribution to managing information in cities (Albino et al., 2015). Nowadays, the goal is not just about managing information, but also about sustainability, quality of life, and efficiency of government and business (Yin et al., 2015). This chapter explains the smart city applications, architecture and infrastructure, to show how and where it is applied.

Key approaches

There are three main approaches to view smart cities, which are also seen as the foundation of a smart city. The organizational approach emphasizes the role of governance in smart cities (Silva, Kahn, Han, 2018). Political choices and the visioning and thinking of local authorities shape the smart city environment (Angelidou, 2014). Bolivar (2015) states that, although governance differs per city, three principles should generally be included. First, a smart city should support in economic development delivery plans of public services. Second, governance should be pragmatic, focusing on practicality, achievability, and financial viability of projects. At last, Bolivar (2015) states that local stakeholders should be involved increases the relevancy of initiatives. These stakeholders are businesses, public institutions and the people in a city. In general, a bottom-up approach seems to be a key factor for smart city governance (Neirotti, De Marco, 2014). The government can adapt the role as coordinator, funder and regulator to make sure that all stakeholders work well together (Bolivar, 2015).

Next, the technical approach emphasizes the role of information and communication technology (ICT) in smart cities. Innovative, intelligent systems are a key characteristic of smart cities (Belanche, Casalo, & Orus, 2016). ICT systems are part of the physical infrastructure, and according to Silva et al. (2018) the quality of the ICT infrastructure has a high impact on smart city performance. For example, creative people might feel themselves more attracted to a city with excelling companies than to other cities (Albino et al., 2015).

Further, the social approach is another way to view smart cities. Investments in social and human capital are expected to result in sustainable growth and an improved quality of life (Belanche et al., 2016). The most important aspects relating to social and human capital are knowledge, inclusion and participation of the citizens in smart city initiatives (Angelidou, 2015). To make sure that smart city initiatives become a success, citizens should be aware, responsible and show commitment towards the initiatives (Silva et al., 2018). To conclude, a smart city is built on organizational, technical and social blocks, thus investing in these aspects increases the value of a municipality's services.

Applications

There are five dimensions (Figure 2) where the smart city principles can be applied. First, smart energy uses sensors to monitor energy usage and generation (Zhang et al., 2017). The goal of smart energy is to incorporate renewable energy sources with other energy sources, to increase sustainability and reduce the negative effects on the environment (Silva et al., 2018). Second, smart living represents applications at home and in the community to increase the security and quality of life (Albino et al., 2015). This could allow a citizen to remote-control his devices and use it for energy-saving, surveillance, entertainment and other purposes (Zhang et al, 2017). Decisions could also be automated based on data, leading to a maximized energy efficiency of homes and other buildings, like warehouses (Silva et al., 2018).

Third, several smart, governmental services increase the city's efficiency. Examples are smart parking, traffic, governance and healthcare (Zhang et al., 2017). Smart healthcare is introduced as a solution to reduce the gap between the demand and supply of healthcare, and to keep it efficient, accurate and sustainable (Silva et al., 2018). Health management becomes more people-centric and real-time monitoring can be established by using networks to keep track of patients (Ismagilova et al., 2019). The main target of smart services is to increase the quality of life.

Fourth, smart environment is currently an important dimension for smart cities. It is based on weather predictions, waste management, water management and monitoring of the city environment (Ismagilova et al., 2019). The importance is high, because of its effects. For example, measuring waste, air, water and gas pollution can increase sustainable development and prevent health issues (Zhang et al., 2017). Further, city trees could damage cables, therefore, monitoring trees might help to prevent damage (Ismagilova et al., 2019).

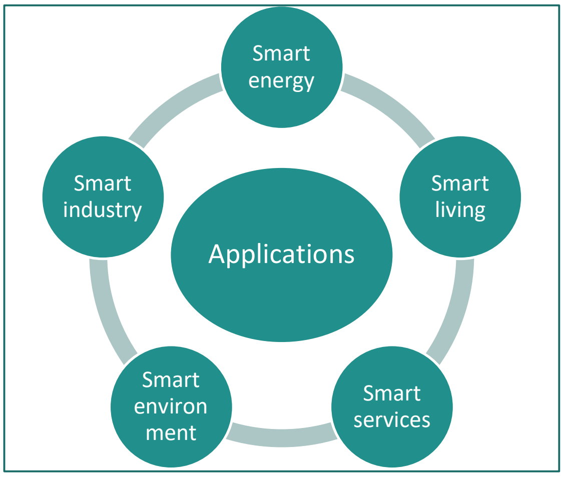


Figure 2 Smart city applications (Zhang et al., 2017)

At last, smart industry could be implemented by organizations, to achieve industrial efficiency. Smart industry is the most influential dimension for creating sustainable development (Zhang et al., 2017). Implementing smart city principles in the business's processes, increases the efficiency of work (Zhang et al., 2017). Soft initiatives could be facilitating in innovative and entrepreneurial activities (Neirotti & De Marco, 2014). Examples of hard initiatives are transportation, buildings, and improving facility management (Neirotti & De Marco, 2014).

Architecture

A smart city consists of multiple components. First, it is instrumented, which stands for the components and devices used by citizens. Second these components are interconnected, being able to send and receive information from a network. Third, smart cities are intelligent, due to the ability to make decisions based on analyzed data (Elmaghraby & Losavio, 2014). These three components are also the three characteristics for smart products, which together form the internet of things (Porter & Heppelmann, 2015) in a heterogenous network with components to monitor and control activities (Zhang et al, 2017).

The internet of things consists of four different layers (Figure 3), which are the sensing, network, data management and application layer (Silva et al., 2018). The sensing layer represents the high number of smart devices which capture the information (Yin et al., 2015). Habibzadeh (2019) states that these often have a low computational power and are of heterogenous nature, which

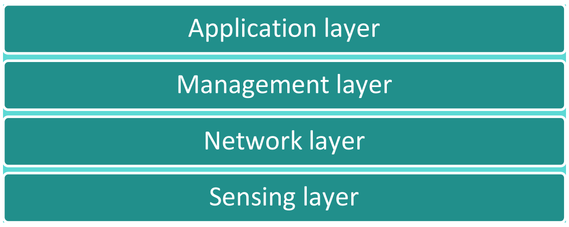


Figure 3 Smart city architecture (Silva et al., 2018)

creates challenges regarding the interoperability (Gharaibeh et al., 2017; Habibzadeh et al., 2019). Second, the network layer uses communication networks, like 4G, Bluetooth or RFID tags to communicate with the management systems of the smart city (Silva, Kahn, Han, 2018). Third, Silva et al. (2018) state that the management layer is used for "data manipulating, organizing, analyzing, storing and decision-making" (p. 702). At last, the application layer refers to the earlier discussed application domains. Sensitive data goes through all of the layers, for example location and health conditions information of citizens (Habibzadeh et al., 2019; Zhang et al., 2017). Thus, all layers have to be secured.

2.2 Cyber security

Cyber security is one of the main concerns of smart cities. It is a way to protect the systems of an organization against malicious and non-malicious cyber-threats (Refsdal, Solhaug, & Stolen, 2015), and prevent negative financial, operational and safety effects (Habibzadeh et al., 2019). The term information security intertwines with cyber security (Elmaghraby & Losavio, 2014). The difference is, that information security focuses on all threats concerning information, like physical, technological and human related threats, whereas cyber security only focuses on information that can be reached via the cyberspace (Refsdal et al., 2015).

There are three main requirements for cyber security. These are confidentiality, integrity and availability (BIO 2019; Elmaghraby & Losavio, 2014; Zhang, 2017). They are in line with the information security goals as defined in the ISO/IEC 27000 series. Regarding smart cities, Elmaghraby and Losavio (2014) also emphasize the importance of the right of privacy and its relating legal and social concepts. Further, Zhang et al. (2017) explicitly mentions the non-repudiation and access control as cyber security requirements for smart cities.

To meet these requirements, cyber security should be taken into account in different management fields of the organization. Since all information is in the cyberspace, a framework about information security applies to this paper, and not just a cyber security framework. Da Veiga and Eloff (2007) proposed a framework to manage information security in an organization. In this framework, they divided information security into six main categories (Figure 4). These categories cover strategic, managerial and operational, and technical management of information security (Da Veiga & Eloff, 2007). Their framework is often used in the field, and a more recent holistic view on information security management shows that their view is still accurate (Soomro, Shah, & Ahmed, 2016). One difference might be that Soomro et al. (2016) see humans as the "most critical element in information security" (p. 220), and Da Veiga and Eloff (2007) put less emphasis on it.

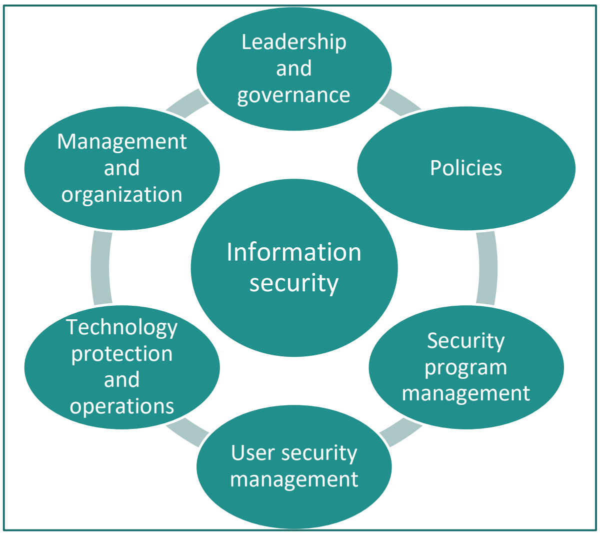
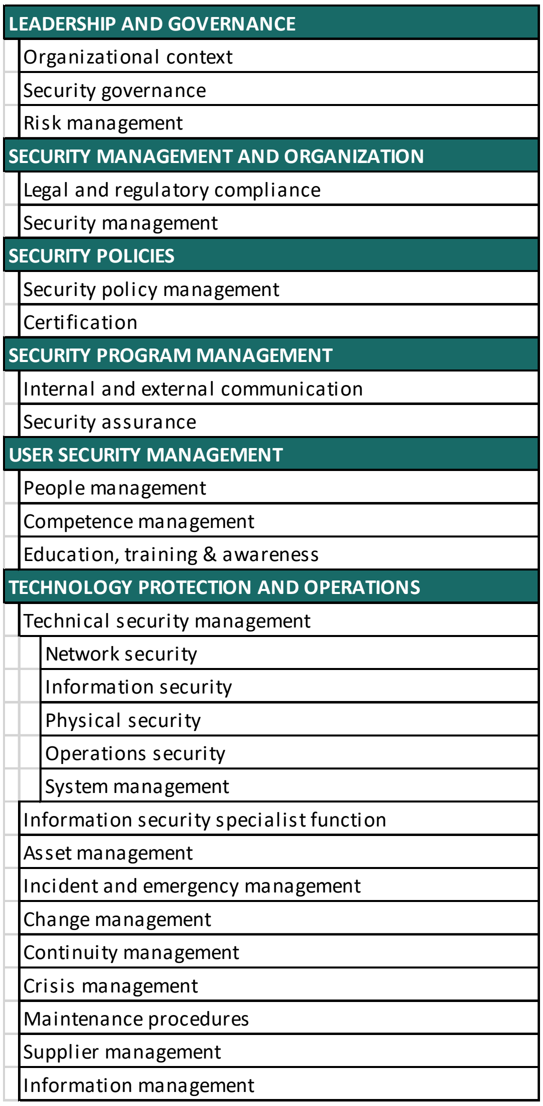

Leadership and governance
Management and organization
Policies
Information security
Technology protection and operations
Security program management
User security management

Figure 4 The six IS categories according to Veiga & Eloff (2007)

The six categories are used as a guideline to compare different cyber security frameworks. Starting off with the first category, leadership and governance describes the role of the board and management to information security (Da Veiga & Eloff, 2007). The role of the board is pivotal in cyber security (NCSC, 2019). The board should set risk targets (BIO, 2020; NIST, 2018) and prioritize them to create a baseline (NCSC, 2019). Furthermore, creating a positive security culture should be considered (NCSC, 2019). Next, security management and organization refers to the organizational design, like the responsibilities, skills, experience and resource levels (Veiga & Eloff, 2007), in favor of the accountability (Von Solms & Von Solms, 2004). Another category consists of the security policies, explaining the corporate policies that can be used by employees as a guideline in their operations (Da Veiga & Eloff, 2007; Von Solms & Von Solms, 2004). Monitoring, compliance and auditing are included in the category security program management (Veiga & Eloff, 2007), to prevent a false sense of security (Von Solms & Von Solms, 2004). This is also stressed in the BIO, stating that activities should be registered, saved and regularly reviewed (BIO, 2020). The next category, technology protection and operations, involves the traditional security of all technical and physical systems (Da Veiga & Eloff, 2007). To maintain a sufficient security level, Dutch municipalities use a checklist to keep systems up-to-date, concerning the topics change management, incident management, patch management and configuration management (BIO, 2019a).



LEADERSHIP AND GOVERNANCE		
	Organizational context	
	Security governance	
	Risk management	
SECURITY MANAGEMENT AND ORGANIZATION		
	Legal and regulatory compliance	
	Security management	
SECURITY POLICIES		
	Security policy management	
	Certification	
SECURITY PROGRAM MANAGEMENT		
	Internal and external communication	
	Security assurance	
USER SECURITY MANAGEMENT		
	People management	
	Competence management	
	Education, training & awareness	
TECHNOLOGY PROTECTION AND OPERATIONS		
	Technical security management	
		Network security
		Information security
		Physical security
		Operations security
		System management
	Information security specialist function	
	Asset management	
	Incident and emergency management	
	Change management	
	Continuity management	
	Crisis management	
	Maintenance procedures	
	Supplier management	
	Information management	

Figure 5 Cyber security categories

At last, the user plays a role in information security as well. The category user security management covers awareness and educational programs, ethical conduct and trust and privacy related topics (Da Veiga & Eloff, 2007). The users of ICT in a municipality are the citizens, managers and directors, employees, IT administrators and suppliers (BIO, 2019b). Human behavior influences cyber risk management in every stage of the process (BIO, 2019b).

Based on these six categories, the NIST (2019), BIO (2020), NCSC (2019) and ISF Standard of Good Practices (2020) are investigated and the results (Figure 5) will be used in a later stage to categorize cyber risks. To conclude, by applying the six discussed categories, an organization can improve the quality of their information security and ensure the availability, confidentiality and integrity of their data.

2.3 Risk Management

Risk management is traditionally seen as the "process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk" (NIST, 1995). Two main standards can contribute to managing risks. First, the National Institute of Standards and Technology published a cybersecurity framework for critical infrastructure, focusing on the cybersecurity threats which might affect the security, safety, economy and healthcare of the United States. The second one, NEN-ISO/IEC 27001, is a standard published by the International Organization for Standardization (ISO) and International Electronical Commission (IEC). Standards published by ISO and IEC are administered by the Dutch standardization institute (NEN). The ISO/IEC 27001 standard is also used by Dutch public organizations.

In The Netherlands, institutions manage their cyber risks in accordance to the Baseline Informatiebeveiliging Overheid (BIO). It is an information security framework for the entire government, based on the NEN-ISO/IEC 27001:2017 standards and published by the Informatiebeveiligingsdienst (BIO, 2020). So, the BIO applies to the national government, regional water authorities and the provincial government. In February 2020, the Informatiebeveiligingsdienst made a further detailing guide about the IoT, because it is indispensable in nowadays' society (BIO, 2020a). Thus, the BIO assists governmental institutions in The Netherlands to cope with existing and new cyber risks.

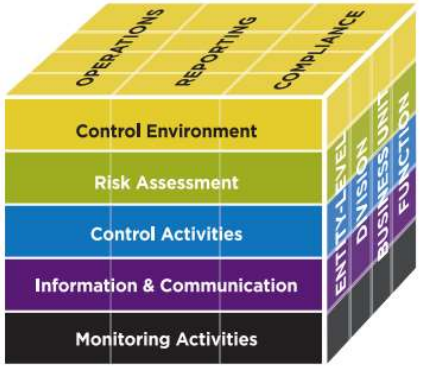


Figure 6 COSO Risk Management Framework

The cyclic process of risk management is often based on the model of The Committee of Sponsoring Organizations of the Treadway Commission (COSO) as depicted in Figure 6. Risk management in the BIO is also based on the COSO model (BIO, 2019). First, a control environment should be created by establishing objectives, strategies and structures to manage risk. This usually is the task of senior management and directors (COSO, 2015). They should understand risk management in the context of smart cities in order to effectively control the risk management process.

Risk assessment is the second phase of the model. ISO (2018) makes a clear distinction in this phase by dividing it into three parts, namely risk identification, risk analysis and risk evaluation. Smart city risks can be identified in the risk identification phase and checked on its relevancy (ISO, 2018). A view on the relevancy of the cyber risks for a municipality can differ per person, for example due to their field of expertise (ISO, 2018). Thus, several experts within the smart city should check for this relevancy of the described risks in this thesis to a specific smart city. The second step in assessing risk is risk analysis, where risks are quantified. In order to quantify risks, acceptance criteria (risk appetite) and measurement criteria need to be defined first. Afterwards, risks can be expressed by the chance of occurrence multiplied by the possible impact, usually resulting in a matrix with low-, medium- and high-level risks (BIO, 2019; Gordon & Loeb, 2003). Third, the risks are evaluated, evaluating the right strategy to manage the risks. Gordon and Loeb (2003) state that risks can be reduced by improving the level of security, or via insurance. Two other ways might be by just accepting the risk or by avoiding the risks (BIO, 2019). In the next phase, control activities from the previous phase are developed to reduce the risk. These preventive or detective activities contribute to mitigating risks, to achieve the risk management objectives (COSO, 2013). Thus, depending on the risk, it will be secured, insured, avoided or accepted.

The information and communications phase stands for the duty to report on risk management practices to internal and external auditors, to check if organizational targets are achieved (COSO, 2015). The monitoring activities phase defines the importance of ongoing evaluations to ensure controls and risk (COSO, 2015). Besides the process, responsibilities are also defined in the COSO (2015) model, explained by their three lines of defense. The first line is formed by the operating managers who own and control the risk. The second line consists of the staff department who monitor risks. Internal auditors represent the third line (COSO, 2015). To relate this to the municipalities, line managers have the task to identify and evaluate risks (risk assessment), control (control activities) and monitor risks (monitoring activities) (BIO, 2019). According to COSO (2015), they should also make sure that they communicate internally and externally, for the purpose of the audits (information & communication). Internal auditors have to check if the organization's goals are accomplished by the usage of the model. Further, the control environment is the director's responsibility, so this might be the responsibility of the councilors and mayors.

3. Methodology

3.1 Cyber risks

3.1.1 Risk factors from literature

The systematic literature review (SLR) is structured based on the guideline of Webster and Watson (2002), which focuses on the information systems field. The first step is to search for papers. Scopus is the search engine used in this research. The following two inclusion criteria are used: (1) The paper should be in a top journal. As a rule of thumb, the journal should be in the top 20% of its category in the InCites Journal Citation Reports of Web of Science. (2) The paper should be published in a journal, fitting in at least one of the following categories of Web of Science: (a) Computer Science, Information Systems, (e) Computer Science, Artificial Intelligience, (c) Computer Science, software engineering, (d) Information Science, interdisciplinary fields, (e) Computer Science, Theory & Methods, (f) Computer Science, Hardware & Architecture, (g) Computer Science, Cybernetics.

This research technique does not cover all relevant papers and respected conference proceedings, because key research papers might be unavailable on Web of Science or were not published in a top journal. Therefore, the citations used by the papers in step one should be analyzed, as well as analyzing the papers that cited the paper in Step 1. A concept-centric data matrix will be provided with uncovered key concepts.

To identify the papers of top journals, search terms should be formulated. Webster and Watson (2002) do not give a specific way to do this, but one way is by breaking down the search string into different facets, followed by a list of similar words (Kitchenham & Charters, 2007). Kitchenham and Charters (2007) state that these similar words can be obtained by checking subject headings of papers, for example by using the reference list of key papers. In order to do so, the reference lists of two literature reviews in a top journal are used as a starting point (Gharaibeh et al., 2017; Xie, Tang, Huang, & Yu, 2019;). This gave the following outcome:

Smart city: smart city OR smart cities
Cyber security: security OR cybersecurity
Risk: issue* OR threat* OR risk* OR vulnerab* OR attack* OR security challeng* OR crime

Full string: TITLE-ABS-KEY (("smart city" OR "smart cities") AND (security OR cybersecurity) AND (issue* OR threat* OR risk* OR vulnerab* OR attack OR crime)) AND (LIMIT-TO (SUBJAREA , "COMP"))

A motivation is given to elaborate on the search terms. First, smart cities cover technologies like the internet of things, which uses machine-to-machine communications and tactile internet, defining human-to-machine communications (Xie et al., 2019). The internet of things is seen as the architecture of smart city, and it goes along with key technologies like cloud computing, network function virtualization, software-defined networking, fog computing, artificial intelligence, big data and information centric networking (Xie et al., 2019). Next, the cyber risk part is covered by two search terms, namely security and cybersecurity. Since researchers are often likely to leave out any further specification of security, it should be kept broad (Gharaibeh et al., 2017). Lastly, synonyms of risks are retrieved from the references of Gharaibeh et al. (2019).

Inclusion criteria	Exclusion criteria
Cybersecurity risks for smart cities	Testing a new tool or prototype (e.g. new authentication or encryption protocol)
Cybersecurity threats for smart cities	Risks for one specific application within smart city (e.g. specific networks testing)
Cybersecurity challenges for smart cities	Papers not going into detail on security (e.g. only mentioning security risks once to introduce paper topic)
	Papers focusing on privacy of data

Table 2 Inclusion and exclusion criteria

Combining these three search terms led to a list of 1189 papers. By filtering on the earlier mentioned top journals, a list of 108 papers remained. These papers are further filtered by reading the introduction and the conclusion (Table 2). The following inclusion and exclusion criteria were used. This led to 22 papers that were full-read for the SLR (Figure 7).

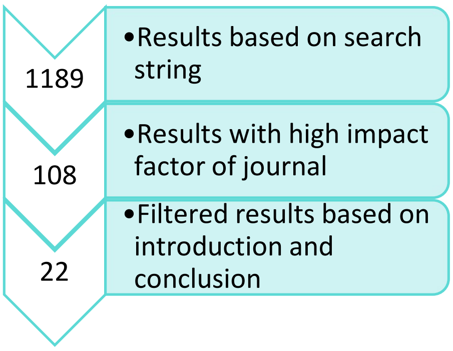
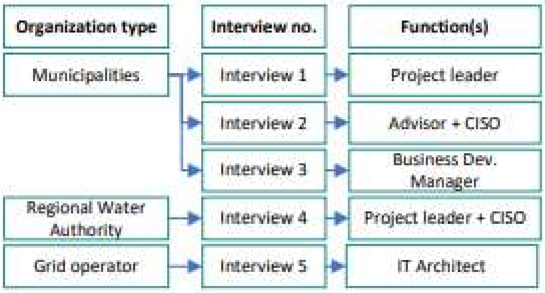

1189
•Results based on search string
108
•Results with high impact factor of journal
22
•Filtered results based on introduction and conclusion

Figure 7 Selection process SLR

3.1.2 Risk factors from interviews

Semi-structured interviews with open-ended questions are organized to find cyber threats and countermeasures which are experienced in practice. The goals of the interview are to find out which cyber risks occurred due to the implementation of smart city applications, which measures were taken in order to control them and how to keep them controlled.

The interviews are coded in order to manage the information that was mentioned. The coding process of Corbin and Strauss (1990) is used. This process consists of three parts, namely open coding, axial coding and selective coding. Open coding is executed to find categories. Transcripts are checked line by line. Next, the interviews are axial coded, by re-reading the text by the self-proposed concepts. Lastly, a table is created with the associated concepts and main categories of interest (Appendix I). It was a deductive coding process, as the theory behind the coding is already investigated in Chapter 2 (Figure 5) (Federay & Muir-Cochrane, 2006).



Organization type	Interview no.	Function(s)
Municipalities	Interview 1	Project leader
	Interview 2	Advisor + CISO
	Interview 3	Business Dev. Manager
Regional Water Authority	Interview 4	Project leader + CISO
Grid operator	Interview 5	IT Architect

Figure 8 Interviewees

Five interviews were organized. Three interviews with representatives of municipalities, one interview with representatives of a regional water authority (representing three regional water authorities) and one interview with a representative of a grid operator. The interviews and the role of the interviewees regarding smart city are displayed (Figure 8).

In order to maintain confidentiality of the interviews, the started projects mentioned in the interviews, are categorized in a separated table (Table 3).

Smart City Application	Type of application	Times applied (max. = 5)
Smart environment	Air	1
	Sound	1
	Nature monitoring	2
	Water	1
Smart living	Smart home	1
Smart services	Governance	2
	Traffic	4
	Parking	1
Smart industry	Facilitating industry	2
Smart energy	Smart grid	2

Table 3 smart city applications

Topic	Sub-topic	Explanation
Source of interview design	*Authors*	Harrell and Bradley (2009)
The research frame	*RQ*	How can smart cities manage their cyber risks?
	Best source	CISO's of smart cities
	Number of respondents	5
Sample	*Convenience*	CISO's willing to help. If no CISO available, SC security officers or SC managers will be asked.
Questions and probes	*Q1*	Which smart city projects are implemented in the organization, or in progress?
	Q2	What is your role within these projects?
	Q3	What are the strategical plans of the organization regarding smart city?
	Q4	How are information security goals and risks set in your organization?
	Q5	Which risk factors, do you think, are important for the information security of smart cities?
	Q6a	Which developments do you expect regarding smart city?
	Q6b	Which effects would it have on information security?
	Q7	Which countermeasures did you take for the smart city applications in use?
	Q8	What support do you expect from an audit and advisory firm, regarding information security for smart cities applications?
Interview protocol	*Introduction*	"I'm a BA-student of the University of Twente, graduating at BDO Hengelo. The purpose of the research is to propose a cyber risk management framework. I have invited you, in order to find SC-specific cyber risks and countermeasures."
	Rules	"The research will take no longer than 1 hour. The information will be used in the master thesis, it will be anonymized, however, it should always be taken into account that someone who knows the city, will recognize the information."
	Questions	See 'questions and probes' section
	Closing	The interview will be translated and transcribed. Some questions might be asked afterwards by the researcher for clarification
	Testing	The interview questions will be reviewed
Preparation for the interview		The systematic literature review should be finished before conducting the interviews. Questions are sent in advance (appendix IV)
Conducting the interview		The structure of the interview will be according to this interview protocol
Capture data		The interview will be transcribed.

Table 4 Interview design smart city representatives

3.1.3 Prioritization of risk factors

The risks are put together as much as possible, and then assessed based on the outcome of chapter 2. Two requirements should be met. First, it should be in line with one of the smart city goals as described in chapter 2. These goals were formulated based on three different approaches, namely the technical, social and governance approach. These goals are displayed in Table 5. Second, it should be in line with one of the smart city characteristics as described in Chapter 2. This gave the following filter criteria:

Governance	Technology	Social	Components
Decision making	Innovation	Quality of life	High number
Economic development	Intelligence	Knowledge	Low powered
Pragmatism		Inclusion and participation	Heterogenous nature
Stakeholder involvement		Awareness and responsibility	Interconnected
			Processing sensitive data

Table 5 Characteristics used for risk prioritizing

3.2 Countermeasures

In order to find the right countermeasures to cover the cyber risks for smart cities, several information sources are used.

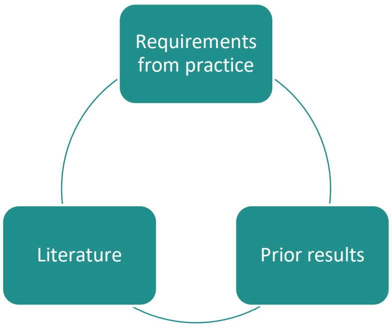


Figure 9 Information sources

First, prior results of this study are used and analyzed again. This consists of two parts. Part one consists of another analysis of the interviews, giving the countermeasures as applied by the smart city. Answers to the following question are used: “Which countermeasures did you take for the smart city applications in use?” In part two, papers of the systematic literature review are analyzed again, to find out if security requirements for smart city applications are already recommended.

Second, current security requirements of public procurements regarding smart city applications are used. These are publicly available, as they are prepared for public tenders. Especially the smart grid is developing rapidly regarding the cybersecurity requirements of IoT devices, and therefore three publicly available documents were used which apply to smart grid operators. The first document contains the Dutch Smart Meter Requirements (DSMR, 2019). This document provides a standard for smart energy meters, to set up open and standardized security requirements (DSMR, 2019). The current version is used, which is version 4.2.3. Second, the security requirements for smart charging proposed by Elaad (2017), a knowledge and innovation center that focuses on the Dutch smart charging infrastructure. Lastly, the German DIN (2019) SPEC 27072 is used, a German standard that contains the minimum cybersecurity requirements for IoT products. In contrast to the other two documents, this standard focuses on the security requirements of smart home devices.

Third, current cyber risk management frameworks from renowned organizations within the industry are used to derive countermeasures. These frameworks are taken into account, because they have a higher focus on management aspects. These frameworks are the Standard of Good Practice by

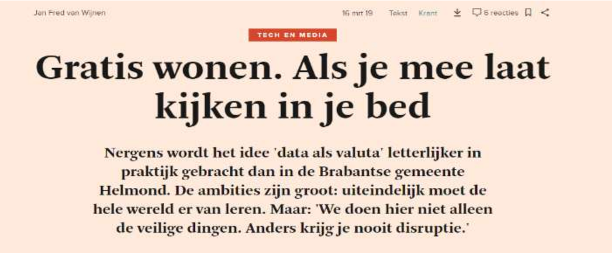
ISF (2020) and the Cloud Controls Matrix by CSA (2019). The framework of ISF (2020) is used because it is a very generic framework, containing almost any category of cybersecurity. The framework proposed by CSA (2019) is used, because it fits to the networked infrastructure of smart cities.

3.3 Validation study

The validation study is conducted based on the theory of Harrell and Bradley (2009) (Table 6). Two experts of BDO were asked about how they think the framework could be used and what could be improved. A profile about the profile of these experts is given. The first of the two participants currently is senior manager on IT audit department, focusing on IT security audits and advisory. ISO 27001 is one of the senior manager's specializations. The second participant holds the position of manager on the IT audit department, being specialized on information security and data privacy. The manager also has prior experience with setting up a cybersecurity framework for smart cities, as she worked on two frameworks for smart city projects in The Netherlands, when she worked for a Big Four audit firm. Due to their theoretical knowledge and practical experience on the topic, they were invited for this validation study. Although they are experienced, the theoretical background of this paper and comments on the framework can be validated with the characteristics as described in Chapter 2, because the number of 2 respondents is low.

Interviewing these experts contributes to getting an understanding about the strong and weak points of the framework, and important factors get more emphasis, and less important factors can be removed. The evaluation form was sent in advance and consists of three parts. First, an introduction is given with information about the purpose of the interview, the questions and background information on smart cities.

The second part contained a newspaper headline with highlights from the article about a Dutch municipality that was exploring the opportunities of smart cities. It gives a view on the opportunities of smart cities, where the question about cybersecurity still had to be asked (Figure 9). Therefore, the experts of BDO were asked if the framework could contribute to the directors and managers mentioned in the newspaper to get an understanding of the cyber risks and countermeasures. The highlights from the article that were mentioned and explained in the evaluation form were: 1) data as currency, 2) Data sensing in homes, 3) Data sensing in public, 4) Collaborations between organizations, 5) Sustainability and 6) Smart energy. This newspaper article describes questionable opportunities for smart cities, which was the decisive factor to use this article, as it invites the interviewees to give their own opinions. The interviewees were asked to use this newspaper as an example for elaboration on the framework, which formed the third part of the evaluation form.



Gratis wonen. Als je mee laat kijken in je bed

Nergens wordt het idee 'data als valuta' letterlijker in praktijk gebracht dan in de Brabantse gemeente Helmond. De ambities zijn groot: uiteindelijk moet de hele wereld er van leren. Maar: 'We doen hier niet alleen de veilige dingen. Anders krijg je nooit disruptie.'

Figure 9 Newspaper headline about conceptual exploration of smart city opportunities

Topic	Sub-topic	Explanation
Source of interview design	*Authors*	Harrell and Bradley (2009)
The research frame	*RQ*	How can smart cities manage their cyber risks?
	Best source	Cybersecurity auditors
	Number of respondents	2
Sample	*Convenience*	Available cybersecurity auditors that have knowledge about smart cities
Questions and probes	*Q1*	How could the framework, according to you, be used in practice?

	Q2	In what way could it contribute directors or managers of smart cities?
	Q3	How could the framework be further improved?
Interview protocol	*Questions*	See 'questions and probes' section
	Newspaper case	https://fd.nl/weekend/1290777/gratis-wonen-als-je-mee-laat-kijken-in-je-bed
Preparation for the interview		A document is drawn up with introductory information about smart cities, a newspaper article which can be related to and the framework itself.
Conducting the interview		The structure of the interview will be according to this interview protocol
Capture data		Notes will be taken and the framework improved. Afterwards, auditors/consultants can check if they agree
Results		Appendix II

Table 6 Interview design validation study

4 Results

The result section contains risk and countermeasures for the cybersecurity of smart cities. The risks are separated in risks from the SLR and risks from the interviews. Then they are combined. Followed by the research on the countermeasures for smart cities.

4.1 Cyber risks

4.1.1 Cyber risks from SLR

The cyber risks retrieved from the SLR are presented (Figure 10). The papers writing about a risk are presented behind the risk, this is done according to the theory of Webster and Watson (2002). The risks are categorized as follows:

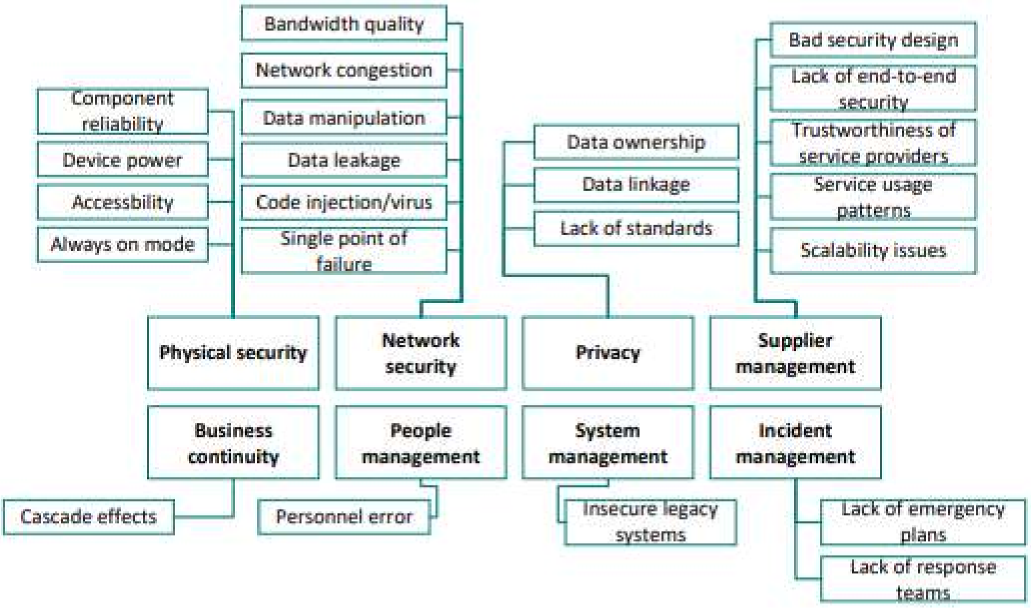


Figure 10 Cyber risks from SLR

Physical security

Reliability of sensor devices should be taken into account. Since these sensors are distributed around the city, reliability is a problem that cannot be avoided (Wan, Lu, Fan, & Lataief, 2017). Wan et al. (2017) state that this can occur when sensors are broken, for example by brute force (Islam et al., 2019) and the wrong data is merged with correctly measured data. Moreover, they could be easily tampered or stolen due to their accessibility in public space (Cui et al., 2018; Minoli, Sohraby & Ochhiogrosso, 2017). A high availability of devices increases the reliability of smart city practices (Badii, Bellini, Difino, & Nesi, 2020). However, bad analysis of the data is not the only reason to keep sensors available. If a device get physically captured, a physical adversary might be able to affect the network performance parameters, such as accuracy, latency and efficiency (Pundir et al., 2020). This is known as a node capture attack, where important information about for example keys can be exposed, impacting the network (Lin, Yu, Zhang, Yang, Zhang & Zhao, 2017). Thus, the institution should be notified in case a sensor device is physically captured. Besides the availability risks, integrity risks also play a role due to the accessibility. Adversaries could also inject malicious code, to use functionalities of the device (Lin et al., 2017). Furthermore, false data could be injected and replaced with correct data, decreasing the effectiveness of smart applications (Lin et al., 2017).

Sensors in smart devices usually have limited power. Latency problems have to be solved in order to use the demanded power of the devices (Islam et al., 2019). Therefore, the lifetime of these devices is often extended by balancing the computational power and energy consumption (Yu et al., 2018). In smart grids, sensor devices also typically have low memory (Islam et al., 2019). Therefore, Diro, Chilamkurti and Nam (2018) emphasize that traditional cybersecurity operations like access control, encryption, authentication and authorization are hard to perform with the smart devices and cloud data centers. And heavyweight security algorithms are not applicable at the device level (Pundir et al., 2020). At the same time, smart cities are sensitive to delays, since applications usually expect a response within a certain time frame (Jan et al., 2019). Thus, smart cities are challenged by resource-intensive operations for low-powered devices. Further, if an adversary breaks into the system, devices could also fall prey to sleep deprivation attacks (Lin et al., 2017).

Network security

Most information in smart cities is processed through wireless networks, therefore the wireless network should be available at all time. However, adversaries might try to disrupt the operations, usually by spoofing or DOS attacks (Diro et al., 2018; Islam et al., 2019). Impersonation is one of the most common spoofing attacks in the IoT-architecture of smart cities, where an adversary tries to eavesdrop information or sniff for the identity of a user, to use another user's identity (Diro et al., 2018; Islam et al., 2019). Man-in-the-middle attacks are another kind of impersonation, but here an adversary gets in between the communication of two nodes, to capture data or authentication information (Diro et al., 2018; Islam et al., 2019). Since the smart city data is characterized as sensitive, data leakage should be prevented. By sending (parts of) the message further to the next node, replay attacks occur (Diro et al., 2018). A node could be tampered and wrong data is sent.

Besides spoofing, DOS attacks might be deployed. It is hard to detect malicious activities, enabling the opportunity to deploy DOS attacks. These attacks bombard the system and make it unavailable by using all data traffic (Lin et al., 2018). This is a severe threat to data security and privacy (Diro et al., 2018).

Attacks are not the only risks for smart cities. The heterogeneity of networks and devices should be taken into account as well. Islam et al. (2019) give different security issues per topology. For example, they state that ZigBee is vulnerable to signal jamming. And the same goes for WAN networks, resulting in drainage of the energy of nodes and unavailable services. Another risk that does not explicitly have to be caused by malicious attack, is the performance on transmission time. Yu et al. (2018) state that transmission time is based on the heaviness of the data and the distance it has to travel. The reliability of public networks should also be taken into account (Jan, Zhang, Usman, Tan, Khan, & Luo, 2019). It could result in bandwidth and latency problems (Yu et al., 2018). Bandwidth and latency issues make it harder for devices to maintain the connection, resulting in battery problems.

The massive amount of collected data is usually stored at third-parties, known as storage suppliers (Yu et al., 2017). This increases the risks, for two reasons. The first reason is related to edge computing, as it is hard to guarantee data integrity when data is split into many parts in the edge of the network (Yu et al., 2017). Second, Yu et al. (2017) state that uploaded data could be modified or abused by adversary users or unauthorized users. Adversaries could reach the data via attacks like eavesdropping, where information can be derived by unauthorized users (Lin et al., 2017). Or cryptanalysis attacks, to derive the encryption key and decrypt data (Lin et al., 2017). The communications have a high impact on the increasing variety of attacks that can be launched on smart cities (Wang, Bai, Lei, Zhao, Yang, Han, 2019). Focusing on fog computing in e-healthcare, Saha, Kumar, Rai, Thomas, & Lim (2019) state that data leakage of privacy sensitive data can occur during data storage or data transmission. Thus, the communication in smart cities leads to risks occurring from attacks, but also due to the heterogeneity and resources of the architecture.

Supplier management

Good data storage and usage is needed to keep sensitive data out of malicious hands. Since institutions are mostly reliant on suppliers, risks are created. For example, a public cloud provider might be able to sell data to his potential customers (Khan, Pervez & Abbasi, 2017). Or when a cloud service provider is infected e.g. by a virus, personal data might be retrieved by an adversary (Saha et al., 2019). Yet, Khan et al. (2017) state that it is unclear when to trust a service provider.

Further, Smart cities are built on heterogenous technologies. The architecture contains heterogenous sources of information, like IoT devices, sensors and streams (Badii, Bellini, Difino, & Nesi, 2020). Furthermore, several heterogenous communications systems are used, which could make it hard to predict where data is generated and how it is made available (Badii et al., 2020). It is hard to scale up the smart city network if security protocols of the network require a lot of modification Pundir et al. 2020). This can especially be hard due to the heterogeneity of the network, containing a large variety of devices, hardware and software (Pundir et al., 2020). Scalability in the smart city network is especially required when larger changes of the network architecture have to occur (Sharma & Park, 2018). The heterogeneity and complexity of the architecture, emphasize the demand for a careful design of the architecture.

Business continuity

Kitchin (2016) wrote about the cascade effects of smart cities. He sees the highly interconnected architecture of smart cities as a vulnerability. When different systems come together, like the energy system and urban operating systems, the one infected entity might be able to infect the other, leading to cascade effects. Besides the interconnectedness of smart devices, Badii et al (2020) see the integration of incident responses as one of the main vulnerabilities for smart cities. Together with insufficient event logging and monitoring, attackers have the opportunity to attack other systems as well.

People management

Cybersecurity risks in smart cities could also occur due a city's employees. For example, when employees open a phishing mail or use an infected memory stick (Kitchin, 2016). According to Kitchin (2016), bad processing of privacy sensitive data is also a risk for smart cities, as anonymisation and security installations might sometimes demand more attention.

System management

Legacy systems might fall prey to cyberattacks. Khatoun and Zeadally (2016) describes the insecurity of legacy systems as one of the challenges for smart cities. The vulnerabilities occur when legacy components that contain old software are not regularly patched (Kitchin, 2016). Kitchin (2016) states that this especially a problem for smart cities, due to the large attack surface.

4.1.2 Cyber risks from Interviews

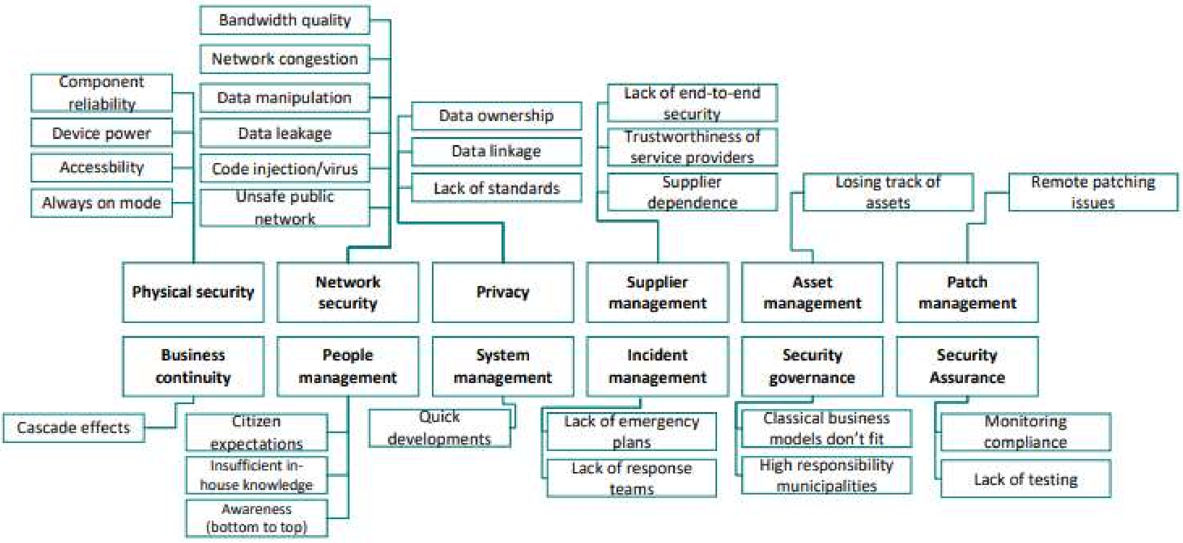


Figure 2

Physical security

Physical security is experienced as an important challenge in practice. It appears that the technology is often complicated. Furthermore, reliable measurements are needed. This could give some issues, as a municipality only had devices available with a deviation of 20%, but needed more precise measurements (interviewee 1, 2020). Further, when trying to find reliable sensors, it should also be taken into account that the devices are expected to last longer than usual IT (interviewee 4, 2020). The interviewee emphasized the difference between operational technology (OT) and IT. Whereas IT, which is mostly used at the office, has a lifecycle of around five years, smart city devices are expected to last for around fifteen years. An interviewee emphasizes the importance of integrity and availability of smart cities, compared to the current focus on confidentiality in current standards like the BIO (int 5, 2020). This shows that reliable components and measurements are important for the functioning of smart cities.

During the interviews it also became clear that the interviewees experienced resource constraints of the smart city devices. Sensors in smart devices usually have limited power (interview 1, 2020). Especially the low battery power is important. The interviewee of int 1 (2020) stated that the municipality is going to implement a narrowband IoT network, to replace the current Low Range (LORA) network. The reason behind this change is the low battery life of the devices. It was expected to be three years, but in the end it appeared to last for only one year (int 1, 2020). If the protocols are not lightweight, an IoT device might not be able to perform as it should.

This is another way of consuming energy resources by an adversary. At last, it should also be taken into account that the lifetime that resources should be available, is longer than usual IT. Because operational technology (OT) has a lifecycle of ten to fifteen years (interviewee 2).

Further, the interviewees told about the accessibility of sensing devices. They are sometimes molested due to wantonness (interviewee 5, 2020). One could also try to manipulate data. Interviewee 1 (2020) gives as an example when someone tries to manipulate sound measurements. However, these manipulations should be executed structural in order to see an effect (interviewee 1, 2020).

Network security

Bandwidth issues and network delays are an important factor for the lifecycle of the battery of devices. An interviewee states that "the LORA-network strength is minimal, a reason why sensors have to work very hard to maintain the network connection" (interviewee 1, 2020). In rural environments this is especially seen as a problem (interviewee 1, 2020). Furthermore, an interviewee sees a strong and reliable network connection as one of the fundaments of the smart city (int 4, 2020). Another interviewee states that delays could also occur due to malicious attacks (interviewee 2, 2020). Further, public networks are not experienced as reliable networks regarding cyber-attacks. For example, an unauthorized party could get access to the sensor device via a telecom network (interviewee 2, 2020). However, this public networks are still used and therefore countermeasures should be taken to prevent code injection (interviewee 2, 2020).

The centralized control over the assets is another risk mentioned in the interviews. Since the control is centralized, it could have a high impact on the infrastructure of a smart city (interviewee 5, 2020). For example, sluices that are controlled via a centralized system, might allow a hacker to open or close all connected sluices if he breaks in the system (interviewee 5, 2020). There are also examples from practice, like the electricity net in Ukraine, which got hacked and firmware was written over the software, making it unavailable for the grid operator (Interviewee 2, 2020). Thus, the interconnectedness could lead to security breaches of high impact.

Supplier management

Like in the literature, the trustworthiness of service providers was considered during the interviews. This got confirmed by interviewee 1 (2020), who stated that trustworthiness is – at least partly - based on a feeling. It is a severe problem in case it concerns critical data, like energy usage or healthcare records. Moreover, supplier management is of high importance since many suppliers are involved in smart cities. In other words, drawing up security requirements for every supplier can be a very time-intensive task. Although it is time-intensive, it should be done carefully. Besides efficiency constraints, suppliers might try to create dependency over certain operations (interviewee 2; interviewee 5, 2020). This is also known as vendor lock-ins. Vendor lock-ins should be prevented, since they can negatively influence the development goals of a smart city (interviewee, 2020). However, setting the security requirements is not so easy in practice, as more knowledge is required than that is available within one organization (interviewee 2, 2020).

Since suppliers have an important role in smart cities, monitoring on the cyber security requirements is essential. However, agreement compliance monitoring is challenging. Agreement compliance monitoring is a structural task, and smart city projects are often funded via traditional business models, with incidental money (interviewee 4, 2020). Furthermore, there is the risk of the bankruptcy of a supplier. This could be a problem if important data is stored at a supplier who is going bankrupt (interviewee 1, 2020). In a business environment with many start-ups, keeping the data available at all times is a relevant challenge.

Reliance on suppliers is a risk that could also lead to patch issues with suppliers. The traditional view on cybersecurity is “if it works, don’t fix it” (interviewee 5, 2020), and as a relatively small organization it might be hard to force patches (interviewee 5, 2020). Whereas municipalities are rather small compared to SCADA developers for example, shows the difference in power during negotiations.

Business continuity

Smart city applications are able to innovate a lot of services. However, there is also a risk in this. If certain services are not applicable for some time, it could result in urban resilience problems (interviewee 4, 2020). An interviewee explains with an example, that an area could be filled with water if one gets access to the control system (interviewee 5, 2020). Or water gets unavailable if water pumps are not working anymore (interviewee 5, 2020).

People management

The interviewees commented on the employees, but also the citizens in smart cities. They do not have the knowledge about smart cities, which creates uncertainties, like “what will happen with my data” (interviewee 4, 2020). And it depends on the type of person – young or old – what he expects from a smart city. But it is not just the knowledge of citizens. Interviewee 1 (2020) states that developments go too quick and that it is too much technical knowledge for one entity to have in-house. This is the reason for the interviewee to outsource all technology regarding smart cities (interviewee 1, 2020). Furthermore, interviewee 5 (2020) put strong emphasis on the awareness of cybersecurity risks throughout the whole organization, by stating that “everything is built on – or – fails by awareness”. Cybersecurity awareness of employees is required to prevent mistakes by employees, for example by connecting an infected phone to the system (interviewee 2, 2020). Besides, awareness by the board is required to get funding (interviewee 2, 2020).

Asset management

Assets might be easy to monitor when they are placed at an office, however, this is in contrast to the many smart devices and sensors placed in public space. When many devices are placed in one city, it might lose track over these devices. After using the sensors, suppliers might not feel any responsibility towards removing the devices after usage (interviewee 4, 2020). This could lead to a high number of devices that are installed on e.g. street lights, of which nobody knows what the actual function of it is and who is responsible for these devices. Moreover, it looks better if it is taken care of (interviewee 4, 2020). Hence, the assets of suppliers should also be managed carefully to keep track over the high number of devices.

Security assurance

The interviewees acknowledge that security assurance needs to be further developed. Suppliers “are always able to say ‘I comply’, but in the end, I think: ‘you intend something different than I do’” (interviewee 5, 2020). It is harder, because standards are missing (interviewee 5, 2020). On the one hand, cybersecurity should be maintained, on the other hand, an interviewee thinks strict rules might block developments. As he states that demonstrable assurance could “flatten developments” if it is involved in a too early stage (interviewee 1, 2020). An interviewee admitted that the front side is checked well on security, privacy and legal aspects, but monitoring compliance to the contracts is a real struggle at the moment (interviewee 4, 2020). In other words, assurance could contribute to making suppliers comply to the rules.

Security Governance

Current governance for smart cities is often not based on policies, but on own considerations. For example, in the Netherlands the BIO is used. However, the BIO mostly focuses on confidentiality of data, since it is focused on secure administrative documents. However, for smart city applications, the integrity and availability of data are very important (interviewee 5, 2020). Sometimes, it is not new technology that is used for smart cities, but it is existing technology used for new goals (interviewee 5, 2020). According to interviewee 5 (2020), this is an insidious risk. Since there are so many new opportunities due to the high amount of data in smart cities, there might also be the risk that all collected data is used for more purposes than it was meant for (interviewee 4, 2020). Whereas one of the discussed smart city goals is to use pragmatic functionalities.

As stated in the previous paragraph, the smart city should govern their risks sufficiently. However, the smart city has several roles within a smart city, namely as a funder, coordinator and regulator. Therefore, a risk could be that information security controls are not sufficiently implemented due to different interests within the smart city (BDO experts, 2020). Sometimes, ethical considerations need to be made. This happens when you are able to connect several data sources to each other. However, there are no policies to comply to, that makes it harder (interviewee 1). This could result in profiling e.g. However, privacy is outside the scope of the research and this will not be further investigated.

Incident management

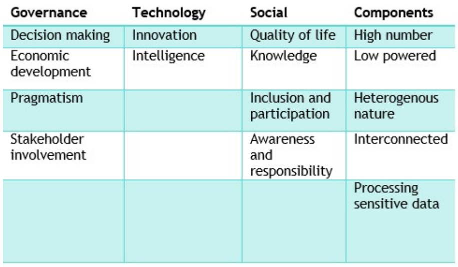
Lastly, incident management has a typical smart city risk according to one of the interviewees. He stated that IoT devices have to managed and secured 24 hours per day. It is expensive for one party to have all technical knowledge and the 24 hours availability over employees (interviewee 5, 2020). Therefore, efficient solutions are required.

4.1.3 Combined and prioritized risks

The prioritization started by adding all risks together (Table 7).

SECURITY CATEGORY	SLR	INTERVIEWS
Physical security		
Device power (battery/computational)	[3][4][9][10][11][12][14][15][22]	[int1]
Accessibility	[1][4][22]	[int1][int5]
Physical reliability/preciseness (longer than usual req)	[12][14][21]	[int1][int2][int5]
Network security		
Bandwith quality/ delays with high computation	[6][10][11][12][14][15][22]	[int1][int4]
Network and device unavailability/congestion	[1][2][3][8][10][11][19]	[int2]
Unsafe public network		[int5]
Data manipulation (sensing/modification/loss)	[1][2][3][6][7][8][10][11][13][15][17][19][21]	[int1][int2]
Data leakage/exposure	[1][3][7][13][16]	
Code injection and viruses	[1][11][13][19][21]	[int2][int5]
Single point of failure issues	[4][6]	[int2][int5]
Supplier management		
Bad IoT security design	[4][5]	
Lack of end-to-end security	[4][7][9][15]	[int2]
Trustworthiness service provider	[7][16]	[int1]
Service usage patterns	[7][8]	
Supplier dependence		[int1][int3][int4][int5]
Scalability issues	[6][10][22]	
Patch management		
Patch deployment issues		[int2][int4]
Business continuity		
Cascade effects	[5][9][21]	[int2]
Level of impact		[int2][int4][int5]
People management		
Personnel error	[9]	
Citizen expectations and knowledge		[int1][int4]
Insufficient in-house knowledge		[int1][int2]
Awareness from bottom to top		[int2][int3][int5]
System management		
Insecure legacy systems	[5][9]	
Security governance		
Classical business models don't fit, board commitment		[int1][int4]
Municipality responsible for all (ethical) decisions		[int1][int4]
Asset management		
Losing track of assets		[int4][int5]
Security Assurance		
Monitoring compliance is a challenge		[int4][int5]
Lack of standards		[int1][int3][int4][int5]
Incident management		
Incident management too expensive for one party		[int5]

Table 7 Risks from the SLR and interviews



Governance	Technology	Social	Components
Decision making	Innovation	Quality of life	High number
Economic development	Intelligence	Knowledge	Low powered
Pragmatism		Inclusion and participation	Heterogenous nature
Stakeholder involvement		Awareness and responsibility	Interconnected
			Processing sensitive data

Figure 11 - recall of table 5

The risks are filtered (Table 8) based on the earlier mentioned characteristics (Figure 11). So they have to be in line with one of the goals of smart cities and one of the component characteristics of smart cities. Furthermore, the results of the validation study are taken into account as well

Interviewees experienced patch deployment issues of their smart city appliances. However, patch management is not included. During the validation study, it turned out that OT has to be patched way less than IT. Therefore it is not seen as a typical smart city risk. Next, people management is excluded as well. Although the importance of awareness of employees and directors has been highly emphasized during interviews, it can be seen as something that is important for any city. This was also one of the outcomes of the validation study. System management is a cybersecurity category that is also filtered out. Data is very important in smart cities, and legacy systems contain around 80% of all data (int 4, 2020). Yet, legacy systems with loads of data do also exist in usual cities and are therefore not in line with the typical smart city characteristics. Lastly, incident management is expensive and demands new solutions, however, the smart city characteristics do not fit to this risk. In the end, five cybersecurity categories are filtered out and its countermeasures will not be further discussed in this thesis.

Filter: IN	Filter: OUT
Physical security	Patch management
Network security	People management
Supplier management	System management
Business continuity	Incident management
Security governance (+ Security assurance)	
Asset management	

Table 8 Filtered cybersecurity categories

4.2 Countermeasures

This chapter gives the countermeasures that were derived from the information sources as explained in Chapter 3. Further, IT controls are given. Smart cities can use IT controls as a guideline for creating security policies. Smart cities can come up with policies to comply to these controls. An overview is given of how the countermeasures are linked to the risks (Figure 12).

C = control description

R = rationale, the goal of the control

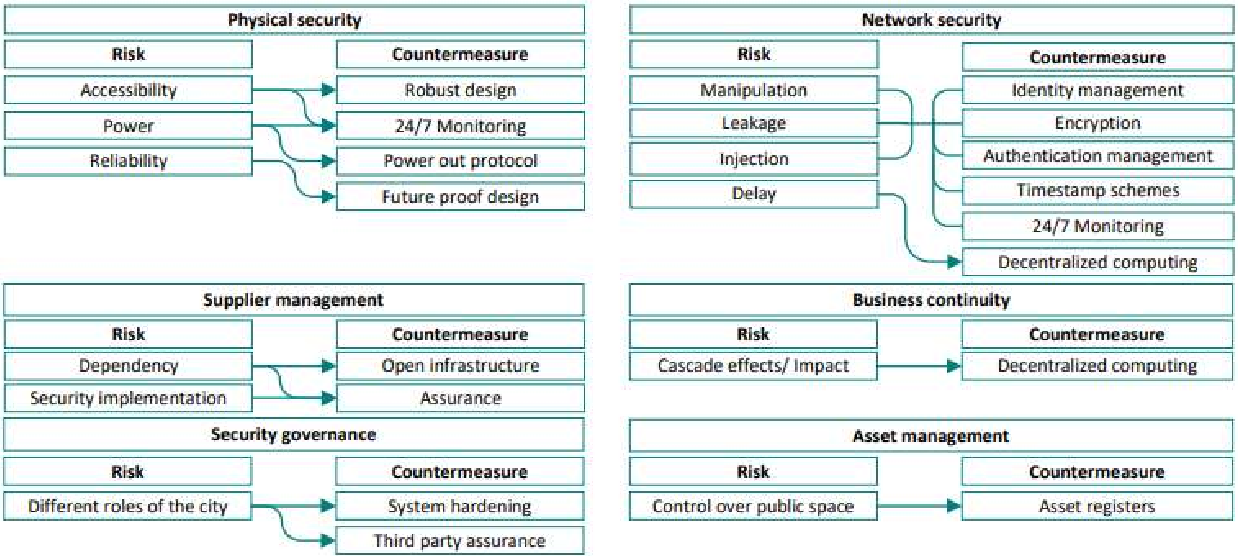


Figure 12 Link between risks and countermeasures

Physical security:

Physical protection

There are three ways discussed in order to control the physical risks of sensing devices. First, a way to control this risk would be by package the device with tamper-proof housing (Pundir et al., 2019). Another way is by implementing a monitoring system. 24 hours per day monitoring can be essential if the data should always be available. Therefore, an Intrusion Detection System could help to check if the devices are physically captured or tampered (Lin, Yu, Zhang, Yang, Zhang & Zhao, 2017). It requires node synchronization in order to design different types of protocols (Pundir et al., 2019). Third, outlier detection could be implemented for analysis, to make sure that the sensors were available over a certain period (Wan, Lu, Fan, Letaief, 2017). In other words, a robust design and notifications on the performance of the hardware could improve the physical security.

Power supplies

Traditional cloud computing and IoT devices are not able to perform reliable security practices. A more efficient way to secure devices, is by using edge computing technology. The location of nodes is with edge or fog computing closer to the end user, which significantly reduces the bandwidth requirements resulting in a decrease of network latency of the cloud (Diro et al., 2018; Yu et al., 2018). Especially fog computing, where the network edge is used as an IoT gateway for computationally complex and intensive operations offloads the device and the cloud. Edge computing is almost the same, but here the edge device is used as a gateway, which offloads the bandwidth of the cloud data center, but still uses power of the sensing device (Jan et al., 2019).

Besides the way data is encrypted and decrypted, another way to deal with resource constraints is applying a future proof design. When components are replaceable, organizations are more easily able to comply to developing security requirements in the coming years (interviewee 2).

Control examples:

C	The physical components of the sensing device must prevent intruders from physical attacks
R	Smart city devices need to be protected against attacks like tampering and physical violation, since they are located in public space.

C	Log events should be created when the smart city device is damaged or accessed by an unauthorized user.
R	The city should stay informed about physical violations and functioning of the devices in order to provide trustworthy analytics. Therefore, changes in the technical status of the device must be .

C	Functionality of sensing devices must not be affected by power outage
R	Power outage should not lead to differences in measurement and settings, and it should start working again if power is available.

C	The vendor must take into account that the design of the device is future proof and security components must be replaceable
R	Memory + computational power should be sufficient for updates, like access control, authentication, encryption (= security functions) Hardware must be replaceable if that's needed for new standards

Network security:

To secure the network against attacks like eavesdropping, Man-in-the-middle (M-in-M-) attacks and denials of service (DOS) attacks, several countermeasures can be applied. Identity management, mutual authentication and encryption enable security enhancement in IoT architectures (Diro et al., 2018). Diro et al. (2018) also proposed a lightweight encryption scheme to do so. This consists of key generation, client encryption, fog encryption and decryption and lastly client decryption. It shows how fog computing can be used in encrypting the services.

Another countermeasure to take is using secure timestamp schemes (Lin et al., 2017). They can contribute to controlling risks of replay and DOS attacks (Lin et al., 2017). Identification, authentication and secure trust management can be possible solutions against spoofing attacks (Lin et al., 2017). Interviewee 2 (2020) stated that authentication mechanisms were also applied to smart devices in critical infrastructure. As well as multi factor authentication, advanced firewalls and the earlier discussed intrusion detection system.

Control examples:

C	Communication between multiple sensor devices must be prevented.
R	Since the devices are interconnected, it should be prevented that one unauthorized user of a smart city device is able to connect with other devices, to reduce the impact.

C	Data leakage must be prevented for the devices, systems and networks that operate with sensitive data.
R	Critical data should be anonymized to make sure that it won't fall prey to attacks like eavesdropping

C	Security keys must be managed, including safe storage and change.
R	Due to the low computational power of devices, cryptography can be an adequate way to confidentially secure these devices. Therefore, cryptographic keys have to be safely managed.

C	The integrity of communicated messages needs to be verified.
R	Due to the connectivity of devices to a network, they are sensitive to attacks. Routines are needed to check the integrity of data input and output and to prevent manual or systematic corruption of data.

C	All privacy sensitive data must be secured throughout the smart city architecture, so that integrity, authenticity, confidentiality, and uniqueness are guaranteed
R	Resource constraints demand low-powered solutions such as cryptography.

Supplier management

Suppliers do not always recognize the importance of information security for smart cities in their products, when priorities differ with smart cities. Involvement in development phase of suppliers, for example by security by design, could assist suppliers to understand which implications come forth with these technologies (interview 5, 2020). In order to find the right security requirements, industry collaborations could be drawn up to set the right security requirements and increase power in negotiations (interviewee 2, 2020). This could also be audited periodically during the lifecycle of the product. Standardization of the security requirements could have a high impact on procurement efficiency, as many suppliers are involved in the process (interviewee 1, 2020).

Keeping many suppliers involved is important. In order to maintain the innovative environment within smart cities, an open infrastructure could help. In other words, an independent party should be able to keep an eye on the interoperability between different suppliers.

Further, smart city networks should be able to grow, by the growing number of devices as well as the security requirements. A security protocol that works for different devices would therefore be important (Pundir et al., 2019). In order to achieve this, decentralized trust management is introduced, which can be globally distributed the concept of globally distributed and locally centralized trust management (Yang, Yang, Lei, Zheng, & Leung, 2018). In other words, this locally centralized way enables authentication and authorization. Another way to do this might be by using software defined networking techniques, which enables control over the network locally (Sharma & Park, 2018).

Control examples:

C	The vendor must prove that sufficient cyber risk mitigating processes have been applied to securely develop the product or service.
R	Trustworthiness is often based on a feeling in smart city projects, since clear laws and regulations are missing. Providing e.g. documentation about penetration tests and employee qualifications about the design phase, would make trustworthiness more tangible.

C	Excessive service usage pattern analysis risks must be taken into account for processing sensitive information
R	Even if all countermeasures are taken, service suppliers might still be able to track sensitive information, for example a cloud provider.
C	External suppliers must not get control over personal data.
R	To ensure public control over sensitive data and the critical infrastructure, the control of external suppliers must be minimized.

C	Security requirements in smart city agreements must be standardized.
R	To keep control over the procurement process, challenges regarding contract management must be managed.

C	Systems must be designed in a pragmatic way, only enabling the functionalities that meet the purpose.
R	Technology (interfaces, ports, device) that is not required for its purpose should be disabled, as well as functionalities of the system

C	The devices and systems in the smart city architecture must provide standardized information, standardized coding and standardized communication channels
R	Due to the many different devices and technologies, systems within the smart city architecture must be designed in a way that they are interoperable with other systems.

Asset management:

Due to the high number of assets it might be challenging to keep track over it. Asset registers are a way to keep track over the assets placed in the public space. This way, one can be sure that suppliers take care over their installed devices and a municipality is able to see whether devices are still functioning properly (interviewee 4, 2020).

Control examples:

C	Devices must be registered in an updated asset register.
R	Since many different devices are installed in public space, an overview of current assets in public space must be deployed to keep track over these devices.

Governance and assurance:

There are many functionalities available for smart applications. Due to the many opportunities it gives, one could lose an eye on the smart city goals. A way to do this is by implementing system hardening protocols. In other words, use a pragmatic approach to decide whether or not functionalities should be available (interviewee 2). However, this is still based on the interpretation of one party, the government. Since the government has several roles, which are funder, coordinator and regulator. Although the municipalities should have a third-party function in the future (interviewee 4, 2020), it is not yet there. As citizens demand support for larger projects and projects are often funded by the municipality (Interviewee 4, 2020). Therefore, smart cities could use third-party involvement to assure that their practices are cyber secure (validation study, 2020).

Control examples:

C	An information security governance framework must be established that is in line with the smart city goals, and commitment to this framework must be demonstrated.
R	Within smart cities, the government can act as a funder, regulator and coordinator. To ensure that these roles do not affect the information security governance, an information security framework should be adapted into practice.

Business continuity

Digital solutions can take over current physical operations. However, this could also lead to reliance on IT. Therefore, an interviewee stated that there should always be an alternative for these critical operations. In other words, redundancy is an important factor in applying smart city technologies (interviewee 4). Besides relying on technology, redundancy should also be kept in mind with supplier contracts. For example, if a supplier goes bankrupt, it should be able to transfer data to keep the data available. Therefore, to continue as a smart city, data should be readable and transferrable to other servers (interviewee 1, 2020).

Control examples:

C	Redundant business solutions should be implemented that ensure business continuity.
R	To make sure that a smart city will not be redundant if it is attacked and critical business can keep on working.

4.3 Validation results

During the validation study, the interviewees were asked to answer three different questions. These outcome is discussed in the section. The outcome is used to improve the cyber risk management framework.

Answers to the interview questions

Q1: "How could the framework be used in practice?"

The interviewees elaborated that the framework could be used in two different ways, for advisory or for assurance. The framework was intended to be an advisory framework by the author. Therefore, the interviewees indicated that it should be used as a top-of-mind study on cybersecurity for smart cities in practice, giving insights in the cyber risks for smart cities. This means that it emphasizes the risks that are key for smart cities, in contrast to the usual risks. It is a management framework, this means that it should not give substantive content to the controls. Lastly, the interviewees emphasized that this framework should be used for governmental institutions, as they are the focus group.

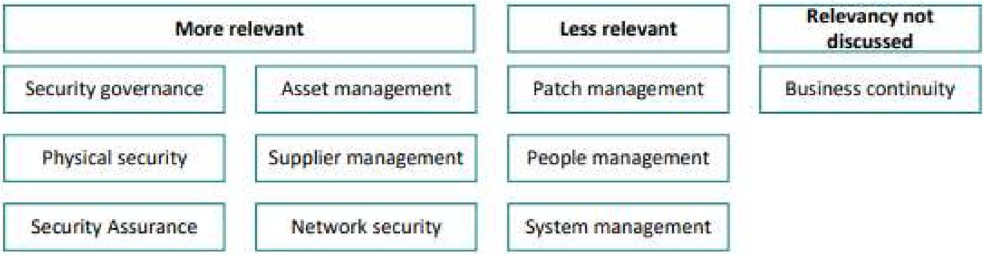
Q2: "In what way could it contribute to directors or senior-managers of smart cities?"

As discussed in the previous paragraph, it gives insights in the smart city risks.

Q3: "How could the framework be further improved?"

It turned out that the cybersecurity categories needed further prioritization in the framework. The interviewees see the 'more relevant' cybersecurity categories (Figure 13) as related to the smart city characteristics. According to the interviewees, security governance, supplier management and security assurance are relevant for smart cities as the smart city typically has several roles within the smart city, as a facilitator, orchestrator and purchaser. This raises several questions. For example, how could a smart city ensure that the privacy of the citizens is guarded? And, how could you ensure that 100% security is one of the premises of a smart city? As an orchestrator, these and other questions should be answered. It also counts for the supplier management, as smart cities have control over the suppliers. Therefore, security governance, security assurance and supplier management are seen as important cybersecurity categories for smart cities.

Besides, physical security, asset management and communication security were discussed as important factors as well. This relates to the high number of connected devices which are typically present in the public space of smart cities. At last, business continuity and privacy were discussed during the validation study. Business continuity was explained, however its importance did not became clear during the validation study. Privacy was discussed as well, but due to the feedback that there should be a clear distinction between security and privacy, the privacy issues mentioned (in for example the interviews) are not further discussed in this thesis.



More relevant		Less relevant	Relevancy not discussed
Security governance	Asset management	Patch management	Business continuity
Physical security	Supplier management	People management	
Security Assurance	Network security	System management	

Figure 13 Risk prioritization results of the validation study

Next to different cybersecurity categories, practical improvements should be clearer as well. First, showing the red line in the framework by connecting different elements. Further, a better distinction should be made between security and privacy, and also between advisory and assurance.

Takeaway for the thesis

In the end, the results of the validation study are combined into three basic principles to improve the framework. These principles are seen as a the requirements for compiling a good framework:

- A top-of-mind framework;
- Smart city focused;
- Connected framework (between different phases of the research).

Next to these principles, the author used the input of the interviewees to prioritize the risks. The experts of BDO see security governance, asset management, physical security, security assurance, supplier management and network security as highly relevant. Whereas patch management, people management and system management are seen as less relevant factors.

5 Conclusion and Discussion

5.1 Conclusion

The main objective of this thesis was to provide an overview of the cyber risks and possible countermeasures for smart cities, structured by the cyber risks management categories proposed by several frameworks. The following research question is answered: *"How can smart cities manage their cyber risks?"*. In order to answer this question, five different sub-questions are answered in this research.

Sq1: "What are smart cities, cybersecurity and risk management?"

First, the concept of smart city is explained. There are three approaches to look at the goals of smart cities. First, the governance approach stands for economic development, pragmatism, stakeholder involvement and improved decision-making in a city. Second, the technological approach emphasizes the urge for innovation and intelligent solutions. Lastly, the social approach represents the aim to improve the quality of life, knowledge, inclusion and awareness of citizens in a city. In order to achieve these goals, smart cities connect the digital world with the physical world by using interconnected and intelligent devices. In contrast to usual cities, where the digital and physical world are not connected, and measurements and decision-making are done in person. By connecting to the physical world, smart cities connect to the critical infrastructure of cities. Besides, privacy sensitive data is processed through the smart city infrastructure. Other characteristics of smart cities, are the high number of devices that are present in the infrastructure, which typically have low-power and are heterogenous of nature. The discussed characteristics are used to prioritize the risks of sub-question 2.

In order to understand how these devices and systems in smart cities can be secured, the concept of cybersecurity should be elaborated on as well. In practice, institutions like NIST, ISF and ISO provide cybersecurity standards to manage organizations. These standards serve as a guideline for organizations to manage their cybersecurity adequately. Within this research, cybersecurity categories are further categorized into six main different cybersecurity categories. These categories can be strategic, managerial or technical. However, to provide a cyber risk management framework, a better understanding on risk management should be provided as well. In this research, this is done based on the COSO (2015) model, dividing the cyclic process of risk management into five steps. This contains defining the risk management strategy, assess the risks, set controls and communicate the performance. Lastly, the performance should be monitored, to find improvements in the risk management cycle. Then, the process start again from the beginning.

Sq2: "What are the cyber risks associated with smart cities?"

Smart cities enrich the opportunities for municipalities, but also increase the attack surface for malicious entities, since devices in the physical, critical infrastructure start to communicate via a network. The cyber risks were derived by conducting the SLR and by interviews with governmental institutions that already implemented smart city projects. Thirty different risks were grouped under the cybersecurity categories from Chapter 2. Seven different cybersecurity categories were kept in this research, as they were highly applicable to the characteristics of smart cities. First, physical security is especially important for smart cities, as many different physical devices are placed in public space, which can be physically accessed and usually have low power. Asset management is also important for not losing track over all these devices. And since they are connected, network security is taken into account as well. It leads to several risks, like bandwidth issues and malicious attacks, resulting in data manipulation, data leakage or viruses. Furthermore, the often centralized cloud environment allows for single point of failure risks, e.g. when many devices are connected via one system that gets hacked. This could have a high impact on a city's infrastructure, thus, business continuity is one of the cybersecurity categories should be managed as well. Next, supplier management is taken into account, as smart cities have to take control over these suppliers. Besides, they often lack a good security design, as low powered devices demand low-computational solutions. Also scalability issues could occur, when different products of different suppliers cannot operate together. Suppliers might try to force these issues, to make sure that cities are dependent on their technology. Thus, suppliers should be managed adequately, as there are many and their priorities might not lie on cybersecurity.

On the other hand, the priorities of smart city management should be questioned as well. Since smart cities fulfil the role of funder, regulator and coordinator, it might be hard to ensure that the highest level of cybersecurity is one of the city's premises. Yet it should not be underestimated, due to the possible high impact of security breaches.

Sq3: "Which factors as discussed in sq2 should be taken into account in a cyber risk management framework for smart cities?"

The cyber risks in the above section were taken into further analysis. Yet, some cyber risks were not, as they were not seen as typical smart city risks. The smart city characteristics as described in Chapter 2 were used to prioritize the risks. Furthermore, the outcome of the validation study also contributed to choosing the right cybersecurity risks. The smart city risks that were filtered out are patch management, people management, system management and incident management. This section will shortly discuss why they were filtered out. First, patch management is important for devices, for example to install new cybersecurity features. This could be a problem, if remote patching does not work, e.g. with older systems which cannot be patched. Yet, it is not taken into account. During the validation study it became clear that OT has to be patched less than IT, and it was not interpreted as a key cybersecurity category for smart cities.

Further, people management not taken into account. Awareness of employees is widely expressed as one of the key cybersecurity categories, but not just for smart cities in particular. Yet, awareness on the specific smart city risks is important to prevent cybersecurity breaches. Another way to look at people management is by looking at it from a citizen point of view. Taking away citizens doubts on cybersecurity could improve a smart city's success, as it might lead to increased participation. However, this is not a cybersecurity risk, but a general governance risk for smart cities and it does not coincide with the smart city characteristics.

Another category is system management, referring to the high amount of data that cannot be extracted from legacy systems. Legacy systems do not represent typical smart cities, as it has nothing to do with the characteristics, and it is therefore left out. The same goes for the last category, namely incident management. Incident management could be expensive for smart cities. An interviewee experienced high incident costs as services should be 24 hours per day available. Yet, it is left out after the validation study, as the critical infrastructure should always be available, even if it is not implemented 'smart'. In the end, these four categories are deleted from the list.

Sq4: "What are the countermeasures regarding the cyber risks?"

Security countermeasures were investigated for every cyber risk in Chapter 4.2. In total, fourteen different countermeasures are elaborated. These can be used as an advice, and it is not an exhaustive list. The risks and countermeasures are linked together in Figure 12. The categories physical security and network security appeared to be important when investigating the risks. Its countermeasures are rather technical, as they focus on improving the hardware and software of the devices. Hardware and software should be managed throughout the whole lifecycle of a product. Furthermore, countermeasures are proposed to keep updated on the functionality within the city, for example by monitoring and protocols when disfunction occurs.

Countermeasures to improve network security are important, but often limited in practice due to power constraints. Lightweight encryption is demanded to use as less computational power as possible. Furthermore, authentication and accesss management is recommended. Several actions could be taken to identify attacks, for example by intrusion detection and firewalls.

Next, is supplier management. In order to maintain the innovative environment within smart cities, an open infrastructure is recommended where new entrants could easily join in. It prevents supplier dependency and stimulates innovation. Further assurance on security measurements in the design process and throughout the lifecycle are recommended. This also relates to the security governance category. In addition, assurance on the practices of the smart city are recommended here as well, due to the different roles of the city. Besides, system hardening protocols could be implemented as well, to ensure that only technologies are used that are favorable for achieving the smart city goals.

Another cybersecurity category discussed is business continuity, focusing on counteracting the high impact security breaches, that could also lead to cascade effects. This could be covered by decentralizing solutions. For example, by setting up smart city projects on a neighbourhood level, instead of city level or larger areas. Or by applying edge/fog copmuting, doing computations at the edge node itself, instead of centralized. This could also prevent data leakage or manipulation throughout the network. An example to do this is by using a public key infrastructure.

Sq5: "Which factors can be added, changed or removed, in order to improve the framework?"

Sub-question 5 is answered by conducting validation study. In order to answer the sub-question, the experts of BDO emphasized to stick to the smart city. In the end, the relevancy of the risks was judged on the cybersecurity category level. Seven cybersecurity categories remained, and four categories were filtered out. Focusing only on the cybersecurity categories that are key for a smart city strengthens a framework. Further, privacy risks were taken out of the thesis. A few were present before the validation study, but they are out of scope and are therefore not mentioned in this research. Further details are covered in sub-question 3.

Main research question: "How can smart cities manage their cyber security risks?"

Smart city is a broad topic, and finding the right ways to manage cyber risks, depends on the projects that are fulfilled within a city. Still, it can be stated that connecting the digital and physical world demands high cybersecurity measurements, to stay redundant as a city. Physical and network security are very important, however, it is often the supplier who produces the products and its security measurements. And as long as standards are missing, as well as assurance on security for smart cities, the city's critical infrastructure is at danger. Smart cities should make sure that security is maintained throughout the design process and the lifecycle of the products. Suppliers need to cooperate in order to secure the smart city architecture from end-to-end. The smart city has a high responsibility in organizing the cyber risk management process, as it serves the roles of funder, regulator and coordinator. To get an understanding of what it takes to manage the smart city, the following framework is presented (Figure 14):

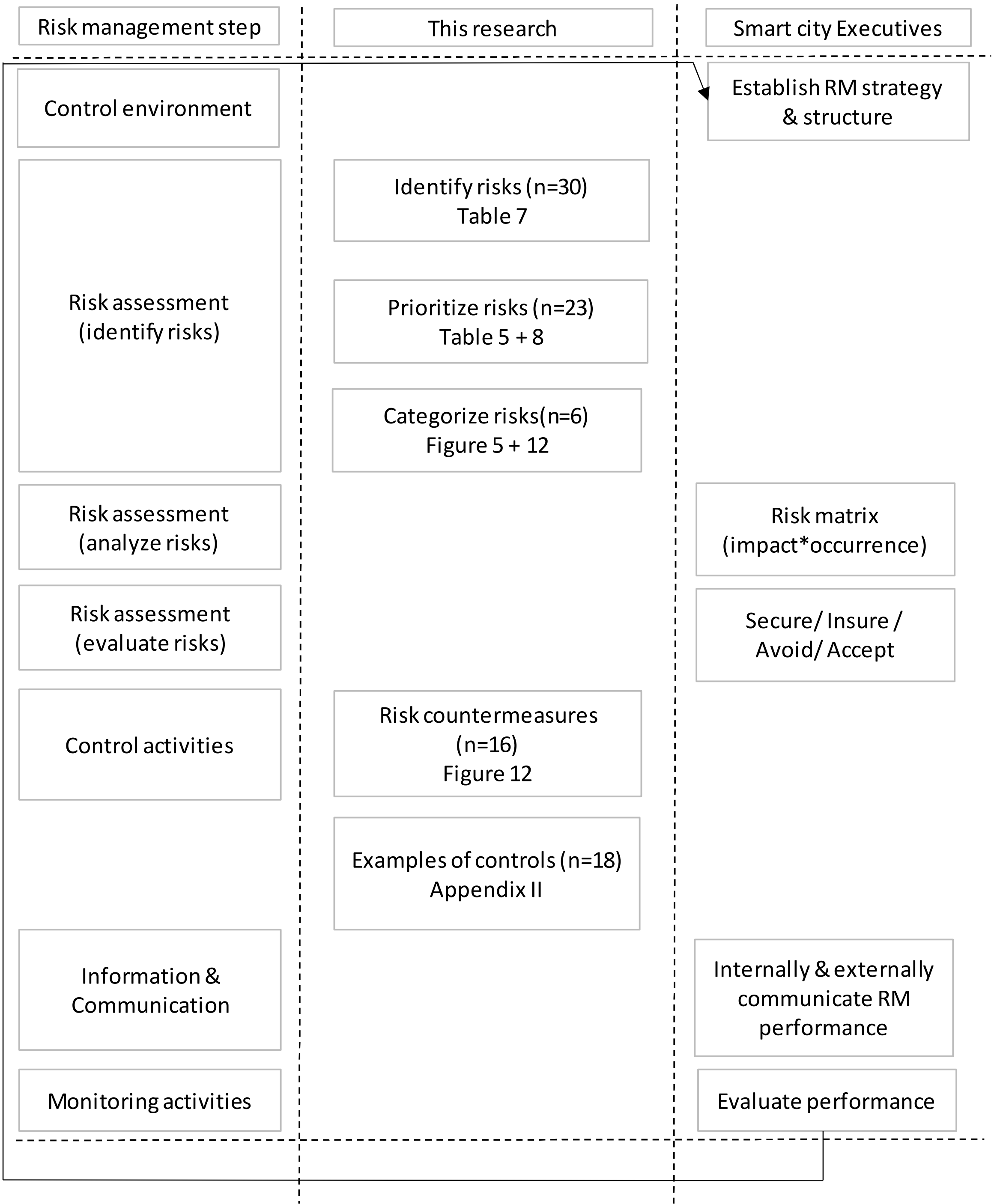

Risk management step
This research
Smart city Executives
Control environment
Establish RM strategy & structure
Risk assessment (identify risks)
Identify risks (n=30) Table 7
Prioritize risks (n=23) Table 5 + 8
Categorize risks(n=6) Figure 5 + 12
Risk assessment (analyze risks)
Risk matrix (impact*occurrence)
Risk assessment (evaluate risks)
Secure/ Insure / Avoid/ Accept
Control activities
Risk countermeasures (n=16) Figure 12
Examples of controls (n=18) Appendix II
Information & Communication
Internally & externally communicate RM performance
Monitoring activities
Evaluate performance

Figure 14 Cyber risk management framework for smart cities

5.2 Practical implications

The risks as discussed in this thesis can be used by (future) smart cities to provide an overview of the cybersecurity risks that are discussed in theory and already experienced from practice. The countermeasures give examples of countermeasures discussed in theory or retrieved from interviews. However, in the end there are many different types of countermeasures, so this thesis should be used for advice only.

5.3 Limitations

This section provides several limitations of this research. First, the research was intended to give a comprehensive insight in how smart cities could manage cyber risks. However, due to the complexity of smart cities, and its many technologies and different ways of applications, it is hard to give a comprehensive framework that would be sufficient to control cyber risks in the smart city architecture in general. However, smart cities demand such a framework, as standards are currently missing. In order to do so, more specification about the research topic would be needed. This was one of the conclusions by the author based on the validation study, changing the approach of the framework from assurance to advisory.

Second, this paper divided smart city applications into five different categories, however, smart industry was not taken into account during the interviews. This research was conducted from a government point of view. This is why smart services, smart environment, smart living and smart energy were discussed during the interviews, but practical findings about smart industry are lacking from the industry point of view. Further, this paper provides many different risks and controls for smart cities, however, the topic of smart city is very broad as governance, technical and social approaches apply to this research. By also taking into account that information security is still a fairly new topic in smart cities, other researchers might find new factors that could contribute to the framework. Next, the framework is validated by experts in the field of BDO Audit & Assurance B.V.. Although all parts of the validation study were discussed, there were still some improvements to be made on the framework. A second validation did not take place, which might have been valuable looking back.

Next, the data sample of five interviews is limited for this type of research. At this moment, there are not many institutions in The Netherlands that express their smart city strategy on publicly available data sources, like the internet. Therefore, it was a challenge to find institutions have been working on smart city projects and were also able to join. Smart city is a broad topic, so more interviews could have led to more new information, based on the difference in projects. Yet, within this research, generalizability was an important factor and in combination with the SLR a comprehensive framework is drawn up.

5.4 Future research

This research investigated the risks and countermeasures smart cities. The next step would be establish policies for these controls, and therefore it would be nice to investigate in future research how this could be established. As mentioned in Paragraph 5.3, a comprehensive cyber risk management framework would be very broad, due to the many different applications and technologies. In order to make a comprehensive framework, one could focus on a specific smart city project in future research and investigate the comprehensive assurance requirements. This is already done in the smart grid, resulting in several requirements for projects like smart meters and smart charging (DSMR, 2019; Elaad 2017)

Another future research point could be to investigate the financial aspect of security. Control activities could be implement, but a smart city could also choose to insure, avoid or ignore risks, based on the financial implications. A research on the financial investments of the proposed control activities would expand the insights in information security for smart cities.

References

Agarwal, V., Patil, R. A., & Patki, A. B. (2019). Architectural Considerations for Next Generation IoT Processors. *IEEE Systems Journal*, *13*(3), 2906–2917. https://doi.org/10.1109/JSYST.2018.2890571

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology*, *22*(1), 3–21. https://doi.org/10.1080/10630732.2014.942092

Angelidou, M. (2014). Smart city policies: A spatial approach. *Cities*, *41*, S3–S11. https://doi.org/10.1016/j.cities.2014.06.007

Badii, C., Bellini, P., Cenni, D., Difino, A., Nesi, P., & Paolucci, M. (2017). Analysis and assessment of a knowledge based smart city architecture providing service APIs. *Future Generation Computer Systems*, *75*, 14–29. https://doi.org/10.1016/j.future.2017.05.001

Belanche, D., Casaló, L. V., & Orús, C. (2016). City attachment and use of urban services: Benefits for smart cities. *Cities*, *50*, 75–81. https://doi.org/10.1016/j.cities.2015.08.016

BIO (2020) Baseline Informatiebeveiliging Overheid. Retrieved from: http://www.informatiebeveiligingsdienst.nl

- BIO (2019) *Handreiking Risicomanagement door lijnmanagers*
- BIO (2019a) *VDW Module 1: Mindmap processen*
- BIO (2019b) *Handreiking Informatiebeveiliging*
- BIO (2020a) *Handreiking IOT Beveiliging*

COSO (2013). COSO Internal Control – Integrated Framework. Retrieved from: http://www.coso.org/

COSO (2015). Leveraging COSO Across the Three Lines of Defense. Retrieved from: http://www.coso.org/

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access*, *6*, 46134–46145. https://doi.org/10.1109/ACCESS.2018.2853985

Da Veiga, A., & Eloff, J. H. P. (2007). Information Systems Management An Information Security Governance Framework. *Taylor & Francis*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136

DIN (2019). DIN SPEC 27072:2019-05 Information technology – IoT capable devices – minimum requirements for information security. Retrieved from: http://www.beuth.de/

Diro, A., Chilamkurti, N., Access, Y. N.-I., & 2018, undefined. (n.d.). Analysis of lightweight encryption scheme for fog-to-things communication. *Ieeexplore.Ieee.Org*. Retrieved from https://ieeexplore.ieee.org/abstract/document/8332478/

DSMR (2019). Dutch Smart Meter Requirements; Main Document, Version 4.2.3. Retrieved from: https://www.netbeheernederland.nl/

Elaad (2017). EV Charging Systems Security Requirements. Retrieved from: http://www.elaad.nl/

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491–497. https://doi.org/10.1016/j.jare.2014.02.006

FD.nl (2020). De wereld deze week: het beste uit de internationale pers. Retrieved on 23 July 2020, via: http://www.fd.nl/

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., & Al-Fuqaha, A. (2017, October 1). Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. *IEEE Communications Surveys and Tutorials*, Vol. 19, pp. 2456–2501. https://doi.org/10.1109/COMST.2017.2736886

Gartner (2018). Gartner Identifies Top 10 Strategic IoT Technologies and Trends. Retrieved from: http://www.gartner.com/

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019, October 1). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, Vol. 50, p. 101660. https://doi.org/10.1016/j.scs.2019.101660

Hassan, A. M., & Awad, A. I. (2018). Urban Transition in the Era of the Internet of Things: Social Implications and Privacy Challenges. *IEEE Access*, *6*, 36428–36440. https://doi.org/10.1109/ACCESS.2018.2838339

Ijaz, S., Shah, A., Khan, A., & Ahmed, M. (n.d.). *Smart Cities: A Survey on Security Concerns*. Retrieved from www.ijacsa.thesai.org

Interviewee 1 to 5 (2020). Interview on the cyber risks and countermeasures. Conducted in the period between 23 June 2020 and 1 July 2020.

Islam, S. N., Baig, Z., & Zeadally, S. (2019). Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures. *IEEE Transactions on Industrial Informatics*, *15*(12), 6522–6530. https://doi.org/10.1109/TII.2019.2931436

Ismagilova, E., Hughes, L., Dwivedi, Y. K., & Raman, K. R. (2019, August 1). Smart cities: Advances in research—An information systems perspective. *International Journal of Information Management*, Vol. 47, pp. 88–100. https://doi.org/10.1016/j.ijinfomgt.2019.01.004

ISO (2018) ISO 31000:2018(en) Risk Management – Guidelines. Retrieved from: http://www.iso.org/

Jan, M. A., Zhang, W., Usman, M., Tan, Z., Khan, F., & Luo, E. (2019). SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application. *Journal of Network and Computer Applications*, *137*, 1–10. https://doi.org/10.1016/j.jnca.2019.02.023

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Khan, Z., Pervez, Z., & Abbasi, A. G. (2017). Towards a secure service provisioning framework in a Smart city environment. *Future Generation Computer Systems*, *77*, 112–135. https://doi.org/10.1016/j.future.2017.06.031

Khatoun, R., & Zeadally, S. (2016). Smart cities: Concepts, architectures, research opportunities. *Communications of the ACM*, *59*(8), 46–57. https://doi.org/10.1145/2858789

Kitchin, R. (n.d.). *Getting smarter about smart cities: Improving data privacy and data security*.

Lim, Y., Edelenbos., J., Gianoli, A. (2019) Identifying the results of smart city development: findings from systematic literature review. *Cities, 95*. https://doi.org/10.1016/j.cities.2019.102397

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, *4*(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200

Michael Porter, by E., & Heppelmann, J. E. (2015). *How Smart, Connected Products Are Transforming Companies*.

Minoli, D., Sohraby, K., & Occhiogrosso, B. (2017). IoT Considerations, Requirements, and Architectures for Smart Buildings-Energy Optimization and Next-Generation Building Management Systems. *IEEE Internet of Things Journal*, *4*(1), 269–283. https://doi.org/10.1109/JIOT.2017.2647881

Mohanty, S. P., Kougianos, E., & Guturu, P. (2018). SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT. *IEEE Access*, *6*, 5939–5953. https://doi.org/10.1109/ACCESS.2018.2795478

Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Current trends in smart city initiatives: Some stylised facts. *Cities*, *38*, 25–36. https://doi.org/10.1016/j.cities.2013.12.010

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). NIST SP800-12 Revision 1 : An introduction to information security. *NIST Special Publication*, (800-12 (draft) revision 1). https://doi.org/10.6028/NIST.SP.800-12r1

NIST (1995) An introduction to Computer Security: The NIST handbook. Retrieved from: http://www.nist.gov

NIST (2018) Framework for improving critical infrastructure. Retrieved from: http://www.nist.gov

NIST (2020) FISMA Implementation Project. Retrieved from: http://www.nist.gov

NOS (2020) 29 Mogelijke datalekken gemeld na problemen met Citrix. Retrieved from: http://www.nos.nl

NOS (2020a) Veel twijfel over corona-app, maar ontwikkeling gaat door. Retrieved from: http://www.nos.nl/

Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J. P. C., & Park, Y. (2020). Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment:

Survey and Future Challenges. *IEEE Access*, Vol. 8, pp. 3343–3363. https://doi.org/10.1109/ACCESS.2019.2962829

Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk management. In *SpringerBriefs in Computer Science* (pp. 33–47). https://doi.org/10.1007/978-3-319-23570-7_5

Rijksoverheid (2020) Securitytest potentiële Corona-apps. Retrieved from: https://www.rijksoverheid.nl/

Rodríguez Bolívar, M. P. (2015). Smart Cities: Big Cities, Complex Governance? In *Public Administration and Information Technology* (Vol. 8, pp. 1–7). https://doi.org/10.1007/978-3-319-03167-5_1

Saha, R., Kumar, G., Rai, M. K., Thomas, R., & Lim, S. J. (2019). Privacy ensured e-Healthcare for fog-enhanced IoT based applications. *IEEE Access*, *7*, 44536–44543. https://doi.org/10.1109/ACCESS.2019.2908664

Security, K. R.-C. &, & 2017, undefined. (n.d.). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Elsevier*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404816301407

Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, *86*, 650–655. https://doi.org/10.1016/j.future.2018.04.060

Silva, B. N., Khan, M., & Han, K. (2018, April 1). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities and Society*, Vol. 38, pp. 697–713. https://doi.org/10.1016/j.scs.2018.01.053

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Szymanski, T. H. (2016). Securing the Industrial-Tactile Internet of Things with Deterministic Silicon Photonics Switches. *IEEE Access*, *4*, 8236–8249. https://doi.org/10.1109/ACCESS.2016.2613512

UN, 2018. 68% of the world population projected to live in urban areas by 2050, says UN. Retrieved from: http://www.un.org/

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers and Security*, *23*(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

Wan, S., Lu, J., Fan, P., & Letaief, K. B. (2017). To Smart City: Public Safety Network Design for Emergency. *IEEE Access*, *6*, 1451–1460. https://doi.org/10.1109/ACCESS.2017.2779137

Wang, D., Bai, B., Lei, K., Zhao, W., Yang, Y., & Han, Z. (2019). Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City. *IEEE Access*, *7*, 54508–54521. https://doi.org/10.1109/ACCESS.2019.2913438

Yang, Z., Yang, K., Zheng, K., Leung., V. C. M. (2019) Blockchain-Based Decentralized Trust Management in Vehicular Networks. IEEE Internet of Things Journal, 6(2), 1495-1505. https:// 10.1109/JIOT.2018.2836144/

Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2017, November 28). A Survey on the Edge Computing for the Internet of Things. *IEEE Access*, Vol. 6, pp. 6900–6919. https://doi.org/10.1109/ACCESS.2017.2778504

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, *55*(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM

Appendix I Coding scheme

1st order concepts	2nd order concepts	Aggregate dimensions
Can't keep up with technological changes	Quick technological developments	Technical security management
Technology is still laborious	Working with new technologies	
Expectations of data outcome of a sensor vs. actual data	Wrong expectations and uncertainties	People management
Citizen should be in control	Citizen involvement	People management
Inadequate level of technology	Quality of technology	Verbetermanagement
Precise measures are a challenge	Data precision and availability	Physical security
Battery failure earlier than expected	Battery capacity	Physical security
Processing capabilities vs. battery	Computational power	Physical security
Privacy in general	Privacy	Privacy
Ethical considerations (gov. support vs citizen control)	Ethics	Privacy
Responsibility issues	Ethics	Privacy
Profiling	Ethics	Privacy
Connecting different sources	Ethics	Privacy
Data linkage	Ethics	Privacy
Laws missing	Ethics	Privacy
Responsibility over data	Data ownership	Asset management
Data ownership should be the citizen	Data ownership	Asset management
Privacy law restrictions	Personal data	Privacy
City has low experience with safe data storage	Data storage	Information management
Security and privacy not tightly regulated for smart city	Rules and regulations	Privacy
Development inhibition by applying certifications too early	Growth potential	Change management
Decision-making based on trust	Stakeholder trustworthiness	Supplier management
Sensors in public space	Data manipulation	Physical security
Multiple devices could be manipulated at once	Data manipulation	Physical security
Unauthorized access	Data manipulation	Access management
Requirements are not sufficient	Supplier agreements	Supplier management
Harder in rural environments	Network availaibility	Network security
Network strength is very decisive in sensor capabilities	Network strength	Network security
Relatively unsafe	Public network/internet provider	Network security
Someone could act like a device	Spoofing	Network security
Protect against firmware	Code Injection	Network security
Reliance on network	Dependence	Network security
Downtime should be mitigated to have valuable data	Downtime	Incident management
Using personal data	Privacy sensitive data	Privacy
City can't keep up with contracts by itself / purchasing efficiency	Contracts	Supplier management
It's too much knowledge for one party / knowledge gap	Knowledge	People management
Different parties should be able to work together	Interoperability	Supplier management
Classical business models don't fit	Business models	Security governance

It is expected that we will have to rely more and more on data and tech	Dependence on technology and data	Change management
Cannot choose the directors of a city, cannot pick based on competences	Competence management	People management
High level of impact	Impact	Incident management
Centralized control over many devices	Impact	Incident management
Too expensive for one organization	Costs	Incident management
Grid applications have been hacked before	Code injection	Network security
Awareness from bottom to top	Awareness	People management
They are expected to last longer than usual IT (10 -- 15 yrs)	Device sustainability	Physical security/Lifecycle management
Devices should be protected to unauth. access when they are connected to network	Unauthorized access	Network security
High size of impact	Critical infrastructure	Business continuity
Only use it for its purpose (expedience)	System hardening	Privacy
It should be patched on distance	Resilience	Patch management
General	Legal	Privacy
Not seeing the value of projects	Board commitment	Security governance
Risk avoiding board	Board commitment	Security governance
Incidental finance for structural costs	Board commitment	Security governance
Fiberglass scarcity	Transmission layer	Asset management
Parties might try to create dependence	Vendor-Lock-ins	Supplier management
Might lose track over assets in the city	Keep control over public space	Asset management
Compliance to agreements monitoring is still a challenge	Compliance	Security assurance
Reliance on their patches against vulnerabilities	Supplier patches	Patch management
BIO doesn’t fit. Standards missing	Current standards	Security assurance

Appendix II List of examples security controls

C = control description

R = rationale, the goal of the control

Physical security:

C	The physical components of the sensing device must prevent intruders from physical attacks
R	Smart city devices need to be protected against attacks like tampering and physical violation, since they are located in public space.

C	Log events should be created when the smart city device is damaged or accessed by an unauthorized user.
R	The city should stay informed about physical violations and functioning of the devices in order to provide trustworthy analytics. Therefore, changes in the technical status of the device must be .

C	Functionality of sensing devices must not be affected by power outage
R	Power outage should not lead to differences in measurement and settings, and it should start working again if power is available.

C	The vendor must take into account that the design of the device is future proof and security components must be replaceable
R	Memory + computational power should be sufficient for updates, like access control, authentication, encryption (= security functions) Hardware must be replaceable if that's needed for new standards

Network security:

C	Communication between multiple sensor devices must be prevented.
R	Since the devices are interconnected, it should be prevented that one unauthorized user of a smart city device is able to connect with other devices, to reduce the impact.

C	Data leakage must be prevented for the devices, systems and networks that operate with sensitive data.
R	Critical data should be anonymized to make sure that it won't fall prey to attacks like eavesdropping

C	Security keys must be managed, including safe storage and change.
R	Due to the low computational power of devices, cryptography can be an adequate way to confidentially secure these devices. Therefore, cryptographic keys have to be safely managed.

C	The integrity of communicated messages needs to be verified.

R	Due to the connectivity of devices to a network, they are sensitive to attacks. Routines are needed to check the integrity of data input and output and to prevent manual or systematic corruption of data.

C	All privacy sensitive data must be secured throughout the smart city architecture, so that integrity, authenticity, confidentiality, and uniqueness are guaranteed
R	Resource constraints demand low-powered solutions such as cryptography.

Supplier management

C	The vendor must prove that sufficient cyber risk mitigating processes have been applied to securely develop the product or service.
R	Trustworthiness is often based on a feeling in smart city projects, since clear laws and regulations are missing. Providing e.g. documentation about penetration tests and employee qualifications about the design phase, would make trustworthiness more tangible.

C	Excessive service usage pattern analysis risks must be taken into account for processing sensitive information
R	Even if all controls are taken, service suppliers might still be able to track sensitive information, for example a cloud provider.
C	External suppliers must not get control over personal data.
R	To ensure public control over sensitive data and the critical infrastructure, the control of external suppliers must be minimized.

C	Security requirements in smart city agreements must be standardized.
R	To keep control over the procurement process, challenges regarding contract management must be managed.

C	Systems must be designed in a pragmatic way, only enabling the functionalities that meet the purpose.
R	Technology (interfaces, ports, device) that is not required for its purpose should be disabled, as well as functionalities of the system

C	The devices and systems in the smart city architecture must provide standardized information, standardized coding and standardized communication channels
R	Due to the many different devices and technologies, systems within the smart city architecture must be designed in a way that they are interoperable with other systems.

Asset management:

C	Devices must be registered in an updated asset register.
R	Since many different devices are installed in public space, an overview of current assets in public space must be deployed to keep track over these devices.

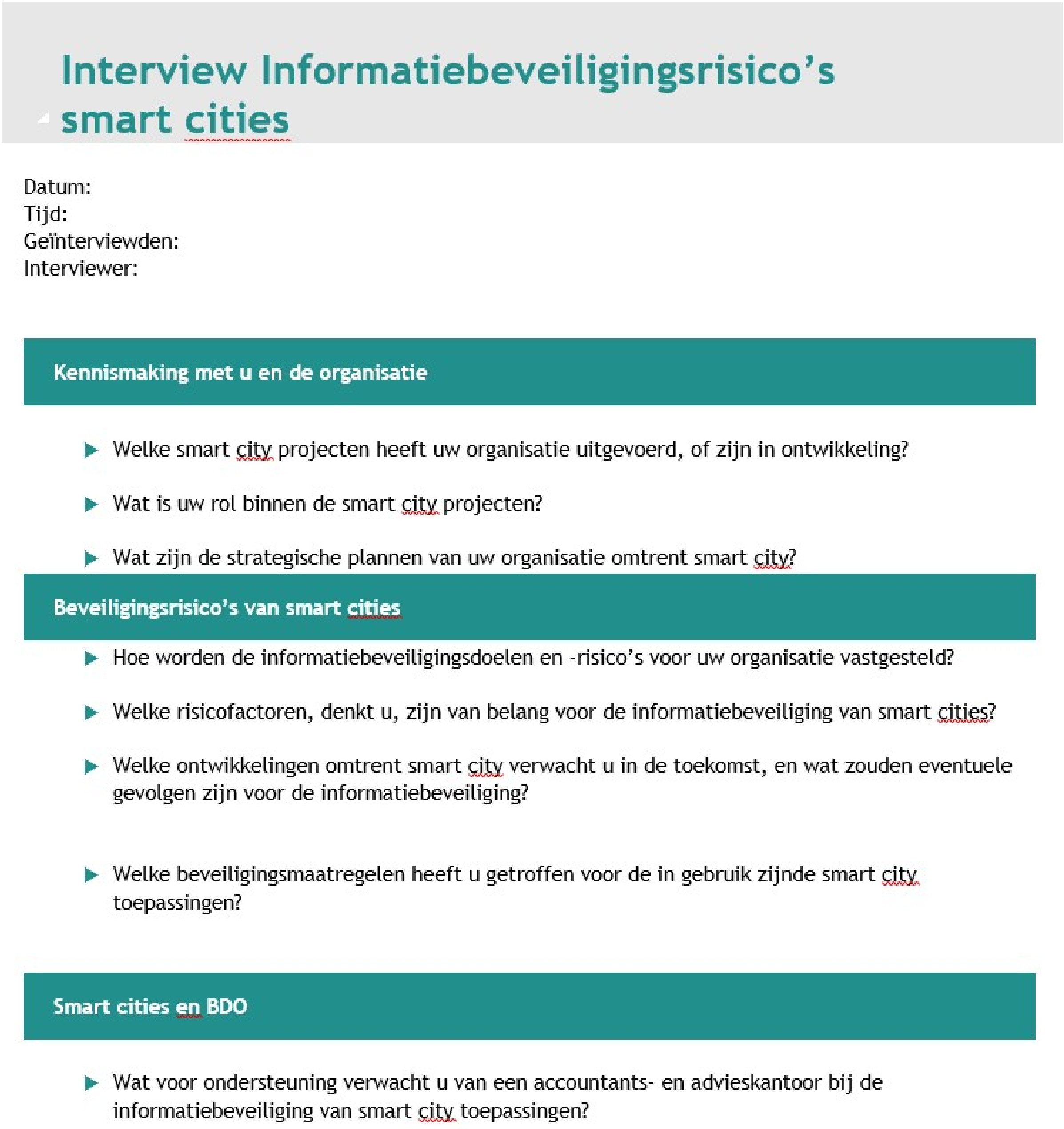
Governance:

C	An information security governance framework must be established that is in line with the smart city goals, and commitment to this framework must be demonstrated.
R	Within smart cities, the government can act as a funder, regulator and coordinator. To ensure that these roles do not affect the information security governance, an information security framework should be adapted into practice.

Business continuity

C	Redundant business solutions should be implemented that ensure business continuity.
R	To make sure that a smart city is not reliant on digital solutions or suppliers for critical operations.

Appendix III Interview questions



Interview Informatiebeveiligingsrisico's smart cities

Datum:
Tijd:
Geïnterviewden:
Interviewer:

Kennismaking met u en de organisatie

- Welke smart city projecten heeft uw organisatie uitgevoerd, of zijn in ontwikkeling?
- Wat is uw rol binnen de smart city projecten?
- Wat zijn de strategische plannen van uw organisatie omtrent smart city?

Beveiligingsrisico's van smart cities

- Hoe worden de informatiebeveiligingsdoelen en -risico's voor uw organisatie vastgesteld?
- Welke risicofactoren, denkt u, zijn van belang voor de informatiebeveiliging van smart cities?
- Welke ontwikkelingen omtrent smart city verwacht u in de toekomst, en wat zouden eventuele gevolgen zijn voor de informatiebeveiliging?
- Welke beveiligingsmaatregelen heeft u getroffen voor de in gebruik zijnde smart city toepassingen?

Smart cities en BDO

- Wat voor ondersteuning verwacht u van een accountants- en advieskantoor bij de informatiebeveiliging van smart city toepassingen?