QATAR UNIVERSITY

COLLEGE OF ENGINEERING

HOLISTIC SMART CITY RISK ASSESSMENT FRAMEWORK

BY

REEM A. AL SHARIF

A Dissertation Submitted to

the College of Engineering

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy in Engineering Management

June 2024

© 2024 Reem A. Al Sharif. All Rights Reserved.

COMMITTEE PAGE

The members of the Committee approve the Dissertation of

Reem A. Al Sharif defended on 26/05/2024.

Prof. Shaligram Pokharel

Thesis/Dissertation Supervisor

Prof. Tareq El Mekkawy

Committee Member

Dr. Farayi Musharavati

Committee Member

Prof. Dinesh Seth

Committee Member

Approved:

Khalid Kamal Naji, Dean, College of Engineering

ABSTRACT

AL SHARIF, REEM , A., Doctorate: June: 2024,

Doctorate of Philosophy in Engineering Management

Title: Holistic Smart City Risk Assessment Framework

Supervisor of Dissertation: Shaligram, Pokharel.

Smart cities are built on the advanced usage of information and communication technology (ICT) in several aspects. Smart city projects are multidimensional and complex. Therefore, risk perspectives need to be considered. Risks are related to privacy and security, infrastructure, standards, governance, and legal.

While these perspectives undoubtedly play crucial roles in shaping the functions of smart cities, there remains a notable deficiency in comprehensive risk assessment. This thesis proposes a holistic smart city risk assessment framework considering both technical and non-technical risks applicable to smart cities. The framework uses an evaluation criterion to help the decision-makers produce and implement risk management plans. Data compiled through interviews with forty persons have been evaluated from risk perspectives and disaggregated into different phases of smart city development and operations.

Based on the framework, the System Usability Scale (SUS) is utilized to evaluate the outputs of the analysis for usability and consistency. The outcome of this analysis shows that the results obtained from risk evaluation closely match the decisions made by the decision makers based on a given environment.

DEDICATION

I dedicate this thesis to all decision-makers working on smart city projects to guide their risk assessment process during all phases of a smart city project.

I would like to thank my parents, husband, daughters, and extended family for their sincere love and continuous support.

ACKNOWLEDGMENTS

I would like to acknowledge the support of my supervisor, Prof. Shaligram Pokharel, for his advice, and continuous guidance during my study.

I want to acknowledge Qatar University for providing all the needs to achieve the requirements of this study.

I affirm that the research presented in this thesis was done by myself. I have designed the questionnaires, collected the data, and developed the analysis method to obtain the results. I am solely responsible for the outcomes and recommendations mentioned in this thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

The smart city idea started taking root in the early 1990s due to the innovation in information and communication technology (ICT) and their increasing use in improving the proficiency and efficacy of business processes, including those in the government sector. An increase in the accessibility and availability of ICT hardware and software helped in planning its adoption for urban processes (Bibri & Krogstie, 2017). Such an adoption can help enhance 'citizens' quality of life, foster the economy, facilitate a process to solve transport and traffic problems through appropriate management, boost a clean and sustainable environment, and provide reachable interaction with the appropriate authority of the government (Ismagilova et al., 2019). Smart cities are expected to be inclusive and benefit their residents (Sanchez et al., 2022). Consideration of other factors, such as laws and regulations, is also important in smart cities (Apostolopoulos et al., 2022). Smart cities also focus on resilience living. In this situation, sustainability includes reducing the use of non-renewable resources, conserving the environment, having a varied and strong economy, autonomous communities, economic strength and variation, independence in communities, citizen well-being, and satisfying elementary human needs.

Smart cities have complex and interdependent systems to provide services to their residents, and there are challenges to such a provision. Such challenges relate to technical, social, economic, and political aspects (Ismagilova et al., 2022). For example, technological interconnection, operations leading to carbon emissions, cost of maintenance and repairs, and data security (Golubchikov & Thornbush, 2020) can be considered as some challenges. Adopting new technology, such as artificial intelligence-enabled devices and operations, might pose challenges during the design and operation stages.

Challenges are also related to risks connected with the implementation and operation of ICT used in smart cities (Golubchikov & Thornbush, 2020). There are risks related to socio-political, financial, technical, partnership, and resource management (Techatassanasoontorn & Suo, 2010); security and privacy (Čolić et al., 2020), and energy systems risks (O'Dwyer et al., 2019). Such risks make smart cities vulnerable in terms of their operations (Mikes,2012).

Similarly, there are associated challenges and risks, such as a lack of standards for smart city applications, a lack of smart 'city regulations and policies, limited integrated solutions, and scarce skilled and critical workforce (Sharma et al.,2020). Therefore, the impact of these risks becomes significant to challenges reduction if they are considered in a smart city project from all aspects: technology, security, privacy, political, environmental, managerial, user trust, and adoption. The assessment can help highlight the potential risks in different aspects of smart city designing and operation (Ismagilova et al., 2020).

The governance of a smart city is another essential aspect that requires effective collaboration between government, stakeholders, citizens, and socio-technical systems. Governance requires a complex framework, policies, and procedures (Ben Yahia et al., 2019).

The provisions of ICT in smart cities promote citizens' participation, enhance growth in human, social, and environmental assets, and create social-oriented smart cities (Bouzguenda et al., 2019). Therefore, smart cities are generally constructed based on four pillars: organizational structure, physical structure, social structure, and economic structure (Silva et al., 2018). Each of these pillars is supported through smart city dimensions. These dimensions help structure the design, plan, program, and policies into a particular dimension and facilitate their interactions through key linkages.

However, these dimensions and linkages are subject to risks as well. Therefore, understanding each dimension and its value in the formation of a smart city becomes important.

1.1 Smart Cities Dimensions

In smart city phases, such as design, planning, and operation, there are six dimensions that are popularly recognized.

Each of these dimensions is discussed next.

1.1.1 Smart Economy

Smart economies comprise guidelines and policies that inspire innovation and creativity in connection with scientific research, innovative technology, and the sustainability concept's attention to the environment(Apostol et al., 2015). Also, a smart economy is defined as the effectiveness of information and communication technologies in the whole economy and the sensible use of assets within the society (Arroub et al., 2016). In a smart economy, technology integrates all disciplines, such as science, industry, business, cultural heritage, architecture, planning, and development(Kumar & Dahiya, 2017).

The smart economy in smart cities takes many forms and applications, some of which are given in Table 1.1. The table illustrates some associated applications to the dimension of smart economy. Forms of the smart economy, challenges leading to non-technical risks associated with each discussed application are also highlighted. Some recommendations in the table are explained to surmount the difficulties.

Table 1.1. Smart Economy Applications

Forms of Applications	Issues\Challenges	Recommendations
Online Platform Economy (e.g., Amazon, Alibaba, Airbnb, and Uber)	• The collection of the information is integrated into the platforms, causing a monopoly in the marketplace. This is considered a challenge for the online platform economy since these platforms can not support complex products(Radonjic-Simic & Pfisterer, 2019). • Platforms function effectively for particular services and products. The platforms do not support organizational requirements. (Radonjic-Simic & Pfisterer, 2019).	The" Distributed Market Spaces" model. is recommended to resolve this challenge. The model is designed to support strategic and operational levels and complex product exchange, and it is applied in smart city information technology infrastructure since the city is characterized by a service ecosystem (Radonjic-Simic & Pfisterer, 2019).
Sharing economy in terms of giving and sharing access to goods and services in a coordinated manner using online services (such as car sharing, bike sharing, room sharing, and sharing services)	• The risk of human behavior is a critical challenge opposing the usage of the sharing economy, as norms and behavior control sharing (Akande et al., 2020).	The government should encourage positive liability and responsibility among citizens to preserve natural resources and enhance smart 'cities' sustainability. The use of the sharing economy concept in renewable energy within microgrids will improve energy consumption and support resilience systems (Akande et al., 2020).
The digital economy fosters digital involvement and engagement for citizens in all aspects of life and encourages digital industries and innovations. Supply chain applications using	• Changing community services to the digital form regarding participation and business procedures at all levels is challenging the application of the digital economy due to a lack of perception of the cybersecurity risk related to IoT applications (Radanliev et al., 2019).	Ensure citizens are engaged, motivated, and skilled to utilize the smart city's digital services. (Carter, 2013). Underpadding risks from all aspects, not considering the standalone situation, and encouraging understanding of different factors' connections and dependencies (Radanliev et al., 2019).

Forms of Applications	Issues\Challenges	Recommendations
Internet of Things (IoT) devices.		
e-commerce service applications, including mobile shopping applications	• Customer data privacy is a major issue for e-commerce service applications (Kirimtat et al., 2020)	Considering ‚users' data privacy is essential, considering the balance between innovations and ‚users' interests. (Kirimtat et al., 2020)

1.1.2 Smart Governance

Governance is the administrative rules, laws, practices, and constraints to manage smart city projects. These projects involve multiple stakeholders; accordingly, improved governance quality is necessary. Smart governance integrates technology, policies, laws, practices, people, and social standards (Arroub et al., 2016).

Smart cities' governance must be allied with the contribution to decision-making, public services, social services, transparent governance, and policies and strategies. Governance is summarized as coordination between citizens and administrative institutions (Silva et al., 2018). By integrating public, private, and civil officials, successful governance will maximize smart cities' benefits regarding consistency, effectiveness, and efficiency of citizens' services. Furthermore, the technical aspect is crucial in smart governance since it assures addressing several city services and features through highly technological solutions (Silva et al., 2018)

Governance is considered the main building block in the collective efforts to develop successful interactions between all actors in smart cities (Nilssen, 2019). Therefore, interactive governance is recommended to promote open innovation. Such an interaction might be facilitated through e-governance (Ismagilova et al. 2019), which can help build transparency in decision-making. Such e-governance can be enhanced using 5G technologies, IoT, and AI. Additionally, cloud-based information services can help decision-making to support participation, engagement, and information sharing for collaborative governance (Ismagilova et al., 2019). Table 1.2 highlights applications, challenges, and recommendations related to smart governance.

Table 1.2.Smart Governance Applications

Forms of Application	Issues\Challenges	Recommendations
Applications to allow users to control their devices within the smart city.	Data security and privacy are major issues faced by the usage of control and social collaboration applications used for smart city governance(Ismagilova et al., 2020; Kirimtat et al., 2020).	• To overcome data security and privacy issues, Decision-makers should be able to grant access based on specific policies and guidelines to ensure 'users' data privacy(Ismagilova et al., 2020; Kirimtat et al., 2020)
Illustrate social collaboration using Information and communication technologies.		• Adopting national policy considering the latest technologies and applications • Introduce an intensive legal framework to increase public involvement (Čolić et al., 2020)
E-government projects and services	The ability of cooperation and support between stakeholders and leadership using e-government services. (Arroub et al., 2016)	• Interaction between people, policies, resources, culture, and information technology to ensure the success of provided services(Arroub et al., 2016)

1.1.3 Smart Living

The OECD Better-Life Initiative framework (*Measuring Well-Being and Progress*, 2022) considers the development and preservation of natural, economic, and human capital as elements of smart living. Smart living is defined as smart structures, including buildings, learning and education, and healthcare (Ismagilova et al., 2019), and is considered an outcome of a smart economy (Apostol et al., 2015). Social perception is another necessary element for smart living that needs to be considered (Silva et al., 2018). Healthcare as an element of smart living can come through real-time monitoring of the needs of the special care and emergency support enabled through the ICT, in addition to home re-habitation applications that were raised during the COVID-19 pandemic to assist medical professionals during this time (Atitallah et al., 2020; Ismagilova et al., 2019; Nižetić et al., 2020).

ICT usage helps smart living through connected and internet-aided computerized living space conditioning, lighting, and connected security systems (Romero et al., 2020). Smart facilitation applications are used broadly in smart homes; they collect intimate and concealed data about their users, yet privacy and security risks are not tackled with precision. Accordingly, risk assessment models are hardly used. It is crucial to set standards and specifications to detect and manage associated risks within smart living applications (Elahi et al., 2019). Empowering technologies such as cloud storage and computing, AI, machine learning, data mining, and wireless sensor networks support smart living applications (Nitoslawski et al., 2019). Table 1.3 illustrates some forms of applications, challenges, and recommendations to overcome the challenges of smart living applications.

Table 1.3 Smart Living Applications

Forms of Application	Issues\Challenges	Recommendations
Smart Buildings	Data security and privacy are the main challenges to the usage and application of smart living applications (Kirimtat et al., 2020)	Applying access control models encourages cryptography and state-of-the-art security architecture. (Vorakulpipat et al., 2021)
E-health systems for smart assistance.		Set specific standards for data security and privacy ((Elahi et al., 2019)
Home re-habitation applications		Adopt transparency in implementing smart city applications (Nižetić et al., 2020)
Smart Tourism		Innovative business models with enhanced security and privacy considerations are required (Kirimtat et al., 2020).

1.1.4 Smart Mobility

The common issues in cities are traffic problems such as congestion, long queues, and delays. Smart systems should focus on using autonomous vehicles and provide coordinated choices for people to ease commutation (Appio et al., 2019). The communication between autonomous cars and smart transportation systems is achieved through IoT devices, which collect real-time road data and route the inspection to potential passengers (Silva et al., 2018). The Internet of Vehicles (IoV) will allow communication between vehicles and support traffic safety, efficiency, and smart mobility(Ismagilova et al., 2019).

The widespread use of IoT in rural and urban areas provides a better-integrated transportation system for smart mobility (Porru et al., 2020). The technologies that enable smart mobility include AI, IoT, big data, and blockchain (Paiva et al., 2021).

Table 1.4 provides several challenges, issues, and recommendations related to smart mobility.

Table 1.4. Smart Mobility Application

Forms of Application	Issues\Challenges	Recommendations
Internet of Vehicle for traffic safety	Availability of Sensor connectivity, the network for the Internet of Vehicles(Porru et al., 2020).	Better integrated systems are used for better services (Porru et al., 2020).
Mobility as a Service, including demand transportation smart ticketing. Road safety and smart surveillance systems	Infrastructure, connectivity, security, and privacy of mobility as a service application (Paiva et al., 2021)	Develop infrastructure, enhance connections, consider security measures, and ensure the existence of policies to govern data privacy(Paiva et al., 2021)
Crowd-assisted smart applications	The availability of real-time connectivity and big data analytics to use crowd smart applications (Ullah et al., 2021)	Use different big data analytical tools to predict peak periods and enhance provided services(Ullah et al., 2021)

1.1.5 Smart People

Smart people refer to a smart 'city's citizens' level of education and societal interaction (Arroub et al., 2016). Smart cities cannot be achieved without the high-level education of their citizens, an open-minded attitude, and adaptive responses to the latest technologies, policies, and laws (Kirimtat et al., 2020).

The social structure of a smart city is primarily related to human and social capital. Human capital is a person's or group's abilities and proficiencies, while social capital is the number and quality of associations linking social organizations. Human and social capital is crucial for improvement, productivity, and smart living in a smart city. Subsequently, higher education institutions such as universities are essential in developing human capital (Ismagilova et al., 2019).

Higher institutes act as knowledge mediators, custodians, and activity providers to support people in becoming smart (Ismagilova et al., 2019). AI and big data are two leading technologies for developing smart applications to enhance knowledge sharing, learning, and teaching (Radu, 2020). However, there might be challenges in accepting the security and privacy of information and services provided to the people (Blanche et al., 2015). Quality assurance has become a critical facet of higher education. People's participation in the state system through IoT is mandatory for the success of the smart city; for instance, an e-government website will grant citizens the opportunity to associate with public services as shareholders and refine it proactively (El-haddadeh et al., 2019).

Table 1.5. Smart People Applications

Forms of Application	Issues\Challenges	Recommendations
Education platforms Social platforms Engaging people with government (e-government platforms)	Data security and privacy are a challenge when using education platforms and e-government platforms(Allam & Dhunny, 2019).	Consider the privacy of information and apply data protection legislation. Spread awareness about smart city applications and cultivate the social community about the advantages of having them(Allam & Dhunny, 2019).

1.1.6 Smart Environment

The smart environment incorporates advances in waste disposal, pollution and energy management, smart grids, house and facility management, air and water quality, increases in green spaces, and monitoring emissions (Appio et al., 2019; Ismagilova et al., 2019). The employment of technology is also essential to sustain natural resources in the cities. Accordingly, to preserve natural resources, sustainable methods to manage them, protect the environment, and reduce pollution are required. That will be through smart energy grids, creating and consuming green energy, and green buildings (Staffans & Horelli, 2014).

The Internet of Data and IoT technologies are used to develop applications related to the smart environment. These technologies use different sensors, such as radio frequency identification, integrated circuits, and optical and pressure sensors, to manage a smart city environment. Collected real-time data will help decision-makers optimize waste and junk collection, recycling, and sorting. Smart environment applications will enhance the decision-making method for the city's logistics and urban strategies (Perera et al., 2014). IoT technologies improve smart city waste-controlling treatments involving electronic waste to support the circular economy (Nižetić et al., 2020). Table 1.6 provides applications, challenges, and recommendations for smart environment application challenges.

Table 1.6.Smart Environment Applications

Forms of Application	Issues\Challenges	Recommendations
Partnership applications between public and private sectors Public consultation in real-time Smart forestry applications	IoT device connectivity issues limit the usage of smart environment applications(Nitoslawski et al., 2019)	Enhancing the infrastructure of smart cities in terms of networks and connectivity. Develop robust AI applications for efficient data analysis and better performance.(Nitoslawski et al., 2019)
Waste management applications		Developing models for sharing infrastructure to reduce cost and increase data sharing between all waste management processes (Perera, Zaslavsky, Christen, & Georgakopoulos 2014).

Forms of Application	Issues\Challenges	Recommendations
E- plants systems for plant monitoring and feedback		Solid planning for smart cities is crucial for better connectivity solutions (Nitoslawski et al., 2019)

1.2 Risks Related to Smart Cities

Smart city development invites risks in multiple areas (Ahad et al., 2020; Coelho et al., 2021). Smart city risks are grouped into three categories: technological, organizational, and external environment (Ullah et al., 2021). Table 1.7 provides a summary of technical and non-technical categories of risks obtained from the literature. Technological risks are defined as the risks related to technology and its employment, such as risks correlated with IoT, big data, and AI, which are the most significant. Technical risks are divided into three general categories in some studies (Singh & Helfert, 2019): network coverage in the city, technology choice, and technology discontinuation. Security risks should be considered in a smart city project; in addition to cybersecurity, attention to risks due to interactions between devices, systems, the absence of supporting infrastructure, unorganized data management, and adaptation of different standards in terms of technology and their integration is mandatory(Ahad et al., 2020) Another technical risk is related to data quality and reliability, specifically with the colossal amount of data produced from systems used in smart cities (D’Amico et al., 2020).

Non-technical risks have an apparent effect on the implementation and operation of smart cities (Ahad et al., 2020). Non-technical risks include governance, legal, and organizational distinctions between public and private segments in smart cities (Löfgren & Webster,2020). Each of these risk categories is described next.

Table 1.7. Summary of Technical and Non-Technical Risks

No	Author	Year	Technical Risks	Non-Technical Risks
1	Ahad, Paiva, Tripathi, & Feroz, 2020	2020	Security risks, high adoption cost, interoperability between different IoT devices, lack of standards	Citizens' mindset and acceptance of digital changes. Natural disasters, such as floods and earthquakes, will affect the infrastructure of smart cities.
2	Ande, Adebisi, Hammoudeh, & Saleem, 2020	2020	Security issues related to IoT systems	
3	Arroub, Zahi, Sabir, & Sadik (2016)	2016	Security and Privacy issues, Interoperability between IoT systems	Lack of standardized laws related to cybercrimes and cyber-terrorism
4	Atitallah, Driss, Boulila, & Ghézala, 2020	2020	Security and Privacy facing IoT applications. Storing big data generated from IoT applications	The cost of infrastructure required to connect all smart city's systems
5	Baig et al., 2017	2017	Cybersecurity, system desecration in smart energy systems	
6	Belanche-gracia, Casaló-ariño, & Pérez-rueda, 2015	2015	Privacy and Security risks in e-government applications	
7	Botello et al., 2020	2020	Security challenges in IoT systems	
8	Caviglione & Coccoli, 2020	2020	Privacy and Security risks in smart	

No	Author	Year	Technical Risks	Non-Technical Risks
			learning in smart cities	
9	D’Amico, L’Abbate, Liao, Yigitcanlar, & Ioppolo, 2020)	2020	IoT Data Security, IoT Data quality and integration	
10	Elahi, Wang, Peng, & Chen, 2019	2019	Privacy and Security risks of different smart systems	
11	Golubchikov & Thornbush, 2020	2020	Cybersecurity and Data Privacy in AI applications in smart cities	
12	Habibzadeh, Nussbaum, Anjomshoa, Kantarci, & Soyata, 2019	2019	Security and Privacy risks associated with smart city technological infrastructure	Policies and governance issues related to smart city technological infrastructure.
13	Hamilton, 2020	2020	Cybersecurity and Privacy risks	lack of policies related to smart cities
14	Ismagilova, Hughes, Rana, & Dwivedi, 2020	2020	Privacy and Security risks for different smart city's applications	
15	Lee, 2020	2020	IoT systems Cyber security risks	
16	Löfgren & Webster, 2020	2020	Privacy and Security of big data generated from smart city systems	Quality standards for the smart city's data Policies of Data Ownership
17	Mehmood et al., 2017	2017	Security, Privacy, and Trust risks of IoT systems Interoperability risks IoT systems	

No	Author	Year	Technical Risks	Non-Technical Risks
			connectivity risks	
18	Mikes, 2012	2012	Operational risks	Legal, ethical risks strategy risks External risks: natural disasters
19	Mohamed, Al-Jaroodi, Jawhar, & Kesserwan, 2020	2020	IoT systems Security, cyber attacks	
20	Neshenko, Nader, Bou-Harb, & Furht, 2020	2020	Cybersecurity risks in smart city systems	
21	Nitoslawski, Galle, van den Bosc, & Steenberg, 2019	2019	IoT device connectivity in smart environment applications	
22	Nižetić, Šolić, López-de-Ipiña González-de-Artaza, & Patrono, 2020	2020	Networking infrastructure risks, Sensors' technological risks	Lack of population education about smart applications
23	Paiva et al., 2021	2021	Risks related to smart mobility Privacy Data Integration and standardization	Environment risks affecting sensors' functionalities
24	Perera, Zaslavsky, Christen, & Georgakopoulos, 2014	2014	Risks of data privacy and security, Lack of standards	Social acceptance, legal issues related to security and privacy
25	Priyanka & Thangavel, 2020	2020	Risks related to big data, in terms of data storage, ownership, security, and privacy	
26	Radu, 2020	2020	Data Privacy risks	environmental impact of e-

No	Author	Year	Technical Risks	Non-Technical Risks
				waste, lack of society adoption risk
24	Sengan et al., 2020	2020	Cybersecurity risks in smart cities	
28	Singh & Helfert, 2019	2019	Technology risks including data privacy and security, the interconnection between IoT devices risks related to network or discontinuing technology	risks related to policies, regulations, and legal guidelines risks related to financial funding of smart city projects risks related to approvals of projects' starting
29	Sovacool & Furszyfer Del Rio, 2020	2020	Privacy and Security risks for smart home applications Devices Interoperability	risks related to costs, and citizen's education and acceptance of technology.
30	Ullah, Al-Turjman, Mostarda, & Gagliardi, 2020	2020	Lack of standardization of Data risk Data security and privacy	
31	Vidiasova & Cronemberger, 2020	2020		risks ignorance of 'citizens' perceptions and smart cities' stakeholders
32	Vorakulpipat, Ko, Li, & Meddahi, 2021	2021	Security and Privacy issues in smart cities' systems	
33	Xie et al., 2019	2019	Security and Privacy of smart cities' blockchain application,	Cost of blockchain applications Lack of regulations

No	Author	Year	Technical Risks	Non-Technical Risks
34	Yigitcanlar, Desouza, Butler, & Roozkhosh, 2020	2020	data storage risks Data Security and Privacy related to Smart Cities' AI applications	related to blockchain unethical recommendations generated by AI applications

1.2.1 Technological Risks

The following sections highlight the dominant technical risks based on the used technology.

1.2.1.1 Technological Risks associated with IoT.

IoT technology is often associated with cybersecurity risks. As the number of connected IoT devices rises to support 'smartness' in various sectors such as transportation, health, energy transmission, and others, its vulnerability to information hacking and misuse also increases. Therefore, the smart city should be supported with measures for cybersecurity risk management(Ande et al., 2020; Lee, 2020).

Cybersecurity issues are not only limited to IoT systems but can also happen due to sensors, networks, and smart city portals (Habibzadeh et al., 2019). Data security and privacy are vital to maintaining the reputation of the smart city and the trust of residents (Mehmood et al.,2017; Sengan et al., 2020).

Infractions in cybersecurity can lead to false alarms, such as fires, earthquakes, or circuit breakdowns, which can endanger the public in the city (Sengan et al., 2020). Therefore, governance causes of security risks and social aspects should be considered when using IoT tools properly. Also, implementing relevant security controls ensures safe data transfer within the smart city infrastructure and the cloud (Baig et al., 2017).

Technical and managerial frameworks should consider resource allocations, in addition to IoT ecosystems and infrastructure, to prevent cybersecurity risks (Lee, 2021).

It is essential to solve the security risks in smart cities holistically and incorporate interconnections between all ICT-related actors: infrastructure, data space, and IoT devices vulnerability (Caviglione & Coccoli, 2020).

Other related risks to IoT technologies are interactions between devices and systems, absence of supporting infrastructure, unorganized data management, and unavailability of universal standards as related risks due to IoT technologies, IoT ethical risks, and the risk of hardware and software failure due to poor design (Mehmood et al. 2017; Kandasamy et al. 2020 ; Sovacool & Furszyfer 2020;) In e-health applications, IoT risks increase because of technical data and applications, infrastructure, and network infrastructure (Zakaria et al., 2019).

1.2.1.2 Technological Risks Associated with AI

Artificial Intelligence (AI) has a significant role in smart cities, businesses, and society. There are various AI applications in smart cities, mainly related to data analytics in energy, education, health, security, transport, sustainable environment, and urban areas management. AI methods are used to develop investigation applications, motion detection, forecasting analysis, threat detection and frauds, crimes, fires, and accident recognitions. The usage of AI applications contributes to the enhancement of all smart city dimensions (Yigitcanlar et al., 2020),

Associated risks with AI applications are security and privacy risks(Allam & Dhunny, 2019). System complexity associated with AI technologies creates technical risks. These risks may create litigations and need many confirmations related to deference with existing laws related to fundamental rights protection (Yigitcanlar et al., 2020). However, risks associated with AI are mentioned in Table 1.8.

Table 1.8. Associated Risks with AI Applications in Smart Cities

No	Smart City Dimension	AI Applications	Associated risks	Reference
1	Smart Economy	Automated data management and analysis will enhance productivity and innovation. Pattern recognition will reduce costs and increase resources. Analyzing big data from multiple resources will improve decision-making. Reaching a conclusion using logical reasoning	Cybersecurity and data privacy	(Yigitcanlar, Desouza, Butler, & Roozkhosh,2020)
2	Smart living	Enhance health monitoring. Improve health diagnosis. Provide independent and interactive tutoring systems.	Data privacy and protection	(Yigitcanlar, Desouza, Butler, & Roozkhosh,2020)
3	Smart Environment	Monitor environmental changes. Optimize energy consumption and production. Enhance functional operations of smart transport systems	Cybersecurity	(Yigitcanlar, Desouza, Butler, & Roozkhosh,2020)
4	Smart Governance	Enhance surveillance systems operations. Aid disaster management. Increase 'citizens' contribution to decision-making.	Cybersecurity	(Yigitcanlar, Desouza, Butler, & Roozkhosh,2020)
5	Smart People	Enhance Knowledge sharing applications. Improve learning and teaching tools	Data Privacy and protection	(Radu, 2020)
6	Smart Mobility	Improve predictions of traffic status, road	Security and Privacy	(Paiva et al., 2021)

No	Smart City Dimension	AI Applications	Associated risks	Reference
		conditions, and streetlights		

AI and Robotic applications in smart cities are used worldwide, such as in Moscow, Toronto, Ottawa, Hong Kong, Dubai, Sydney, New York, and London, and yet, social risks need to be considered, in addition to cybersecurity and data privacy risks (Glouchkov & Thornbush 2020).

Mitigation of AI risks can be achieved by the incorporation of blockchain and other encryption technologies with AI, which can help to define asymmetrical behavior, identify the threat, and control it rapidly to assure data security within the smart city system (Botello et al., 2020; Priyanka & Thangavel, 2020;Yigitcanlar et al., 2020).

1.2.1.3 Technological Risks Associated with Blockchain

Blockchain technology is considered a solution for security challenges related to IoT technologies. Blockchain technology is based on a point-to-point decentralized network where all transactions are validated by registered nodes and stored in a central ledger. This characteristic of blockchain is utilized to build a network to enhance data security within the IoT system (Botello et al., 2020). The adoption of blockchain technology within smart city dimensions has peripheral threats and risks, including security and privacy, low productivity, storage, and energy intake efficiency (Xie et al., 2019).

Blockchain technology is used to create autonomous governance platforms for smart cities to dissipate transparency related to privacy and cost efficiency. Such a platform will minimalize security and privacy risks in smart 'cities' applications (Coelho et al., 2021).

Some of the applications of blockchain on smart city dimensions and main risks are given in Table 1.9.

Table 1.9. Associated Risks with Blockchain Applications in Smart Cities

No	Smart city Dimension	Blockchain Applications	Associated risks	References
1	Smart Living	Smart health applications for healthcare providers and medical researchers as a storage repository for chained medical data Medical data access control to ensure access for authorized users	Data security and privacy	Xie et al., 2019
2	Smart Environment	Storing Electricity consumption information using smart contracts to enable automatic payments.	Data security and privacy Low productivity	Xie et al., 2019
3	Smart Mobility	Implementing a decentralized smart transport system Facilitate electricity trading for electric vehicles using Blockchain smart contracts	Data security and privacy Energy consumption efficiency	Xie et al., 2019
4	Smart Economy	Sharing services using blockchain-based technology to ensure availability, confidentiality, and integrity	Low productivity	Sun, Yan, & Zhang (2016).
5	Smart Governance	Decentralized governance tool for smart cities to manage digital assets using blockchain technology.	Data security and privacy	Coelho, Oliveira, Tavares, & Coelho, (2021)
6	Smart People	Smart social communication applications using blockchain technology to avoid cyber attacks	Data Privacy	Sadik, Ahmed, Sikos, & Najmul Islam,(2020)

1.2.2 Non-technological Risks

The following sections will illustrate non-technical risks: socio-economic, governance, legal and strategic risks.

1.2.2.1 Socio-economic risks

Socio-economic risks include the traditional mindset of stakeholders and decision-makers. Implementing the smart city concept means handling multidisciplinary projects that require a considerable budget, trained personnel, and technology exposure to the citizens, decision-makers, and professionals. For instance, in smart grids, social risks involve the general proposition of specific technology. There is a need to examine social struggles on smart grids and the future of electricity systems because these systems involve different actors: regulators, customers, technology companies, and energy service providers for better efficiency, sustainability, and cost control (Meadowcroft et al., 2018).

Other social risks are associated with the neglection of citizens' observations and other stakeholders' participation in smart cities. Ineffective community involvement will affect a smart city's capability to provide an increased quality of life and efficiency (Vidiasova & Cronemberger, 2020).

Also, the effect of the culture of failure assumptions on entrepreneurial activities related to IoT is a main socio-economic risk. This culture may reduce or reject these activities, specifically with the lack of institutional support for individuals with smart city innovations due to associated risks with such initiatives (Kummitha & Crutzen 2019).

1.2.2.2 Governance and Legal Risks

Smart city projects face governance risks involving socio-political risks associated with policies, laws, rules, and political and social forces. Concerns related to approvals of smart city projects, competence in monitoring, resource management, and stakeholder management are some of the factors that should be considered in governance (Singh & Helfert, 2019). A low level of decision-making involvement in solving technology is a main risk since it will lead to reduced intentions to finance smart city projects and threaten the sustainability of current smart cities (Vidiasova & Cronemberger, 2020)

There is a relationship between technical and non-technical risks, such as governance and cybersecurity risks in e-government projects. The main issue is the limited attention given to cybersecurity risk by high-level management. Implementing efficient procedures to safeguard critical systems from cybersecurity risks is important to avoid cybersecurity risks, which requires good cooperation between all sectors. Clear policies and procedures are crucial to articulate prevention and protection measures for these risks. (Malhotra et al., 2017).

Constitutional issues related to data privacy and protection risks arise within smart city projects. Security and privacy issues become prominent when the legal system is not updated to address the issue of technology use, integration, and dissemination of information. The use of close-circuit television in the city, automated bank teller machines, city coverage with wireless frequency, e-payments and transactions, and collection of personal information can be examples of legal instruments that are to be established through analysis. Therefore, sufficient qualities should be formed to assure the public of the security and privacy of data and legal procedures in support of the victim in case of a breach (Hamilton, 2020;Singh et al. (2020); Xie et al. (2019)).

Ethical standards concerning data privacy in smart cities, clear ownership policies for data, and approved standards for data storing, protection, and safety are essential to prevent governance and legal risks (Löfgren & Webster, 2020).

1.2.2.3 Strategic Risks

Strategic risk in smart cities emerges when the strategic approach lacks the link between urban ICT development and sustainable development agendas. The lack of this linkage will condemn ICT investments and increase environmental and socio-economic concerns (Bibri & Krogstie, 2017). Smart city management should discuss tactical risks and difficulties in strategy formulation and implementation. The Strategic risks related to smart city administration or as a project are not explained explicitly in studies. Yet, management must identify generalized unforeseeable threats related to the organization's strategy and operation (Bibri & Krogstie, 2017).

1.3 Purpose and the Scope

Research shows that technical risks are generally considered when designing and implementing smart cities. The focus on non-technical risks is underrepresented. Non-technical risks are complex as they focus on human behavior. Therefore, mitigating the impact of such risks becomes more necessary as the impact of such risks can vary. Based on this, further research should focus on understanding the different types of non-technical risks, in addition to technical risks and their implications, to ensure the effective functioning of smart cities.

Different assessment tools are introduced to assess smart cities concerning operation smartness, sustainability, or management (Deveci et al., 2020; Fernandez-Anez et al., 2018 ;Patrão et al., 2020). Further research can focus on developing better smart city assessment tools suitable for holistically assessing smart city dimensions and using the required procedures to increase performance. From a risk assessment point of view, the existing risk assessment and management methods are not comprehensive (Alawad et al.2020; Dimitriadis et al.2020; Domingos et al. 2008). The available tools lack adequate consideration of non-technology-related risks; technology risks are examined independently (Singh & Helfert, 2019). Also, it is crucial to consider risks in all dimensions and their interrelations since these dimensions are not separated in real scenarios (Zheng et al., 2020).

Therefore, this thesis aims to develop comprehensive research on the risk factors, individual assessment methodologies, and technology and non-technology-based risk. The proposed framework will integrate advanced management methodology and risk assessment theories, which are used as advanced uncertainty analytical methods, to calculate risks precisely and provide evaluated scenarios that will support smart city management's decisions regarding risk management and mitigation plans.

1.4. Objectives and Research Questions

Risk assessment tools and techniques that are explicitly used for risk assessment and management in smart cities are discussed in the previous section. A limited number of risk-related tools are designed specifically for smart cities. However, these tools are designed for a specific application within one dimension and lack comprehensive handling of different types of risks in all dimensions. Therefore, there is a partial understanding of the risk impact in smart city applications, so there are only a limited number of risk assessment frameworks. The absence of a comprehensive risk analysis framework hinders risk mitigation and management (Neshenko et al., 2020). Therefore, the two main objectives of the thesis are as follows:

1. Explore risks and their analysis techniques used in the literature for assessing risks and mitigating the impact of such risks.
2. Propose a generic risk analysis framework and evaluate its applicability in smart city design and operation.

The following are the research questions based on the objectives mentioned above. The first two research questions are related to the first objective, and the second two are related to the second objective.

RQ1: What risk types are applicable in a smart city project?

RQ2: Are there any interrelations between different types of risks?

RQ3: What should be integrated to develop a generic risk assessment framework for smart city projects?

RQ4: How should such a risk assessment framework be applied to assess risk in a smart city design, planning, implementation, and operation?

1.5. Thesis Organization

This chapter introduces the smart city and smart city dimensions. The risks related to each dimension are also provided.

In Chapter 1, conventional technical and non-technical risks related to the adoption of complex ICT in smart cities are also specified. The chapter also provided the purpose, objectives, research questions, and contributions. In Chapter 2, a review of the literature is provided. The review focuses on risk assessment methods, application of management theories, probabilistic graphical models, and decision-making techniques. In Chapter 3, the methodology used for this research and the proposed risk assessment framework and analysis methods are provided. In Chapter 4, data collection and the analysis of such data in relation to the framework are provided. In Chapter 5, the conclusion, contribution, and a list of future research directions are provided.

CHAPTER 2: LITERATURE REVIEW

While planning for a smart city, understanding dimensions and associated technical and non-technical risks becomes essential. Without a good risk assessment and monitoring, the operation of a smart city may not be successful. Risk assessments are to be done through different tools, resulting in a certain strategy to mitigate risk impact. As the smart city is multidisciplinary, the best approach would be to independently associate risks for each project in each dimension (Helfert et al., 2015). Researchers have proposed certain general assessment tools, such as the Smart City Project Assessment Matrix-SC(PAM), a general risk assessment tool that uses project actions aligned with the risks related to a particular smart city dimension (Fernandez-Anez et al., 2018). Other tools are also used for analyzing different aspects of smart city: for example, ISO 37120 for city services and quality of life, ISO 37122 for sustainable development, ETSI indicators for the performance of digital multi-service cities, ITU 4901 to assess the use of ICT in resilience smart cities, ITU 4902 KPI for the influence of using ICT in sustainable smart cities, and ITU 4903, and UN SDG 11+ indicators for measuring the achievement of UN sustainable development goals in smart cities (Patrão et al., 2020).

Frameworks are also used for smart city planning. For example, a framework is developed to value smart cities from eight aspects: management and organization, governance, technology, economy and finance, sustainability, data analytics, community engagement, and institutional context (Deveci et al., 2020). These frameworks are used in smart city decision-making since they are used in risk and challenge prioritization.

In this chapter, risk assessment methods and frameworks are discussed to understand the techniques used and consider risks, smart applications, and dimensions.

Applications of management theories are explained since they will benefit the research by providing a method of comprehensive understanding (Elçi & Çubukçuo, 2014). Accordingly, an understanding of risks, including non-technical risks, in addition to the understanding and prediction of human beliefs of probabilities and impacts of risks, will be achieved.

The probabilistic graphical models are illustrated since they are powerful in modeling uncertainties, risks, and dependencies(Spehr, 2015). The probabilistic graphical models will be used in this thesis to build risk scenarios that may occur during a smart city project.

Then, multicriteria decision-making methods are elaborated since these methods provide a complete evaluation of complex problems, especially when multiple factors are considered. They are also used in risk management and can be used to integrate qualitative and quantitative data, which is crucial for this research(Taherdoost & Madanchian, 2023).

2.1 Risk Assessment Methods

Researchers have focused on specific tools for risk assessment for a definite purpose. Such risk assessment tools may or may not be applicable when the comprehensiveness of the smart city is considered.

2.1.1 Failure Mode and Effect Analysis (FMEA) method

One of the most popular methods to assess risk is the basic FMEA. This method is used mainly in evaluating the critical potential risk to support risk management in a project (Domingos et al.,2008). FMEA is a qualitative method used for risk mitigation during the design phase of a project. It assists engineers and project managers in identifying failure modes, causes, and effects during and before occurrence.

Accordingly, risks can be mitigated early in the project (Roghanian & Mojibian, 2015). Subriadi & Najwa (2020) use improved FMEA as an ICT risk assessment approach. The improved FMEA has four main phases: determining risk assessment requirements, identifying risks, assessing risks, and analyzing and evaluating risks. The exact parameters used in this technique are based on the risk impact category and are aligned with the failure effect. The used parameters are risk severity and time of occurrence. The study concluded that the improved FMEA provided more consistent results, and risks were assessed efficiently.

Failure Mode Effect Analysis (FMEA) is also used in the smart city context (Kandasamy et al., 2020). The main advantage of FMEA is evaluating critical and potential risks to support risk management in a project (Domingos et al., 2008). The FMEA is used in security risk assessment as it can help to differentiate critical failure modes, problems, and conditions affecting the system's hardware and software from safety, consistency, and maintainability (Kandasamy et al., 2020).

The main limitation of FMEA is that it is a qualitative method where risks cannot be estimated unless integrated with other techniques, such as the risk priority number technique that calculates risks using three conditions: occurrence, severity, and detection (Roghanian & Mojibian, 2015).

2.1.2 Monte Carlo Simulation Method

The Monte Carlo simulation method presents the outcome from a sequence of events. The main advantage of this method is its suitability for estimating outcomes from the product of multiple random variables, including sources of uncertainty. The method uses a mathematical formulation to provide results based on random variables that affect the outcome. Each variable is valued from a defined range of alternatives, and the outcome is calculated (Ayres et al., 2017). The limitation of the Monte Carlo method is the computational requirements to run even a simple simulation (Hemantha &.Herathb, 2018).

The Monte Carlo method is used by Hemantha &. Herathb (2018). The study evaluates the quality of IT security investment in organizations due to the importance of such investments in information technology projects. This study could apply to smart cities since they include multiple information technology applications and systems. The authors suggested combining the Monte Carlo method, Markov chain, and Bayesian model to achieve a detection model applied to e-mail intrusion detection. (Hemantha &.Herathb, 2018).

2.1.3 Fuzzy Logic Theory

The fuzzy logic theory defines some transitional values between 0,1, unlike Boolean logic, which strictly results in 0 or 1. Thus, there is no precise true or false evaluation. Values are between sharp evaluations like absolute true and false. The theory is developed to deal with commonly faced concepts in daily life, which makes it resemble human thinking. Fuzzy logic is based on fuzzy sets containing elements with membership levels. An element can be a member of different sets with different values. The difference between probability and fuzzy logic is that probability estimates values about specific reality, whereas fuzzy logic denotes membership in an ambiguous set (Kayacan & Khanesar, 2016).

The fuzzy logic theory is used in smart city risk assessment. A study by Ullah (2018) focuses on risk assessment for underground applications in smart cities, including underground railways, water supply systems, sewerage systems, parking, and electricity lines. The study aims to create one risk index for all the systems, although each has different risk factors and indices. The author used three models to create and measure the generated final risk index: linear approximation, hierarchal fuzzy logic, and a hybrid model based on a combination of both models. The results for the third model to efficiently estimate the final risk index were promising. The resulting model can perform automatic clustering based on the risk index and assist maintenance teams in prioritizing their tasks. The author highlights the need for further research in risk estimation and assessment.

Alawad & Kaewunruen (2020) investigate smart risk assessment methods in railway applications. The authors introduce a risk assessment framework called an intelligent system for managing risks (ISFMR) to increase security and safety and assess and manage risk effectively. The study uses an adaptive neuro-fuzzy inference system (ANFIS) to enhance risk management. AI trained through artificial neural networks (ANN) is used to predict risks and uncertainties based on actual values and risk information.

The study's findings show the precision of the risk level performing estimates with the AI model's capabilities to learn, make projections, and acquire risk level values in real time. The limitation is that the risk assessment tool is the time needed for machine training and the assumption of linearity of the input parameters.

2.1.4 Game Theory

Game theory illustrates multiple people’s decision scenarios, represented as a game. The primary entity of this theory is the players who will take actions and decisions. Each player chooses the action that will result in their benefit. The game includes interactions, constraints, payoffs, and actions taken by the players. Based on the theory, the game will be played by applying the best strategies and estimating the outcomes. The game needs to consider consequences, and the relationship between consequences and players' actions becomes essential to developing an outcome. The ideal state of equilibrium is Nash equilibrium, where the steady state of the game is reached (Song et al., 2020).

Game theory's advantages are flexibility and its wide applications in different disciplines. Limitations to the theory appear when applied to information systems security because of a limited database of related games of network security. The players in this game are the hackers, network infrastructure, and the network administrator. The study by Song et al. (2020) proposed a security approach where players can start moves simultaneously;. However, it may be hard to keep track of moves, and the flow of the game may change with each move, the approach provides a determination of the best time to take action (Song et al., 2020).

Game theory is used for security risk assessment in smart medical devices by Abie & Balasingham (2013), who introduced an adaptive security risk assessment framework to predict damages from related risks to e-Health smart systems. The model needs to operate on a continuous basis by accumulating information on managing risks, monitoring security, and making predictions (Abie & Balasingham, 2013).

Game theory is also used for security risk assessment in cloud computing systems (Furuncu & Sogukpinar, 2015). It is used for security risk assessment with two competing actors, the attackers and the defense system. The application of theory in this study helps formulate an optimal strategy to help decision-makers take the proper security measures.(Furuncu & Sogukpinar, 2015).

2.1.5 Dempster Shafer Theory

Dempster-Shafer Theory is a generalized discrete probability theory in a finite space. It was developed initially by Shafer (1976) by extending the work of Dempster (1967). In this theory, the probability of one possible event is assigned to mutually exclusive sets (Sentz & Ferson, 2002).

Traditional theories assign a probability to one possible event. Still, in Dempster-Shafer's Theory, probabilities can be correlated to multiple possible events, for example, calculating the probability of event A to occur over the subjective probability of event B (Certa et al., 2017).

Three crucial functions construct the Dempster-Shafer theory; the first function is the basic probability assignment function, which is donated by (*m*), the belief function (*Bel*), and the plausibility function (*Pl*). The belief function (*Bel*) refers to the degree of confidence for one event relative to the individual probability of a related event. The basic probability assignment (*m*) or the mass function is the mathematical presentation of the belief function (*Bel*). Plausibility (*Pl*) is the quality of possibility to believe. Plausibility supports the evidence of the belief.

Dempster-Shafer theory is used for security risk assessment in a study by Sun et al.(2006). It can be used for security risk assessment for smart city applications. The authors developed a risk analysis approach, depending on the evidence reasoning approach. The advantage of using this theory is incorporating security risk factors, interrelations, and countermeasures (Sun et al., 2006).

Another study by (Eduardo et al., 2021)concentrated on modeling uncertainties in IoT applications; the author mentioned that Dempster- Shafer theory is used to determine uncertainties in sensor data. Combining the theory with complex event processing provided a better understanding of ambiguities, even in the case of conflicts between sensors' data. The results showed that Dempster–Shaver theory is flexible and effective in dealing with conjectures.

A study by (Ghosh et al., 2020) used Dempster -Shafer theory to detect faults in Sensor data fusion for IoT applications. The authors used the theory to combine data from sensors to make a decision concerning the sensor's faulty status from a data perspective. The study resulted in accurate data when tested in the laboratory and compared to the literature.

A study provided the use of the Dempster-Shafer theory to manage uncertainties in expert systems. The author mentions that the theory is suitable for valuation-based system uncertainty. Other researchers highlighted the usage of Dempster -Shafer theory in determining uncertainties in transportation systems (Awasthi & Chauhan, 2011), determining financial and audit frauds, and providing a risk assessment framework (Srivastava et al., 2011), and modeling uncertainties in GIS systems (Delavar & Sadrykia, 2020)

The main advantage of using Dempster-Shafer's theory is its flexibility in design to handle information precision and systems' uncertainty without further assumptions (Gan et al., 2020). Accordingly, this research will use the theory to analyze multiple risks facing smart city projects.

Table 2.1. Risk Assessment Methods and Theories

No	Theory	Characteristics	Reference	Advantages for use in this research	The disadvantage of use in this research
1	Dempster Shafer theory	A mathematical model to define uncertainty.	(Sentz & Ferson, 2002)	Probabilities can be correlated to multiple possible events.	Unreliable results in highly conflicting multiple pieces of

No	Theory	Characteristics	Reference	Advantages for use in this research	The disadvantage of use in this research
		Used for discrete and interval data. Related to traditional probability theory and set theory. Ability to combine various evidence types from several resources		Flexible design to handle levels of precision of the information and can represent the uncertainty of systems without further assumptions. (Sentz & Ferson, 2002)	evidence. (Gan et al., 2020)
2	Game Theory	Game theory provides a mathematical model of stakeholders’ interactions. Based on two players Used in multidiscipline.	(Soltani et al., 2016)	Flexibility and wide applications in different disciplines(Song et al., 2020).	Limited database of related games, both players can start moves simultaneously, it may be hard to keep track of moves, the flow of the game may change with each move, and it in the precise determination of the best time to take action (Song et al., 2020)
3	Failure Mode Effect Analysis (FMEA)	A systematic procedure to determine failure modes, causes, and effects. Rank failure models are created by combining severity, occurrence, and detection.	(Certa et al., 2017)	Evaluating critical and potential risks to support risk management in a project (Domingos et al., 2008).	Qualitative methods are used where risks cannot be estimated unless integrated with other techniques. (Roghanian & Mojibian, 2015).

No	Theory	Characteristics	Reference	Advantages for use in this research	The disadvantage of use in this research
		Severity, occurrence, and detection have equal weights. Different evaluations of severity, occurrence, and detection may lead to the same risk priority number.			
4	Monte Carlo Simulation method	A mathematical formula that provides the outcome based on random variables. Simple simulation needs complex computational requirements.	(Ayres et al., 2017)	Suitability for estimating outcomes from the product of multiple random variables, including sources of uncertainty. (Ayres et al., 2017)	Complex computational requirements (Hemantha & C. Herathb, 2018)
5	Fuzzy Logic theory	Defines some transitional values between 0,1. Thus, there is no precise true or false evaluation. Needs to be combined with other methods to provide precise indications.	(Kayacan & Khanesar, 2016).	Can deal with commonly faced situations in real life. (Kayacan & Khanesar, 2016).	No precise parameter values must be combined with other methods for better results. (Ullah, 2018)

The previous sections presented different risk assessment methods and theories. The Dempster-Shafer theory can be used as a risk assessment methodology. The beliefs perceived by smart city designers, planners, implementers, and operators provide a basis for assessing risk occurrence, usually based on the absorption of technology in the country, the availability of technology, legislation, and skills.

The theory is scalable and can be applied to a higher number of inputs from planners or experts through the pairwise comparisons of the analysis. As the theory is not based on the scale of the city, it should be applicable in other smart city planning.

2.2 Risk Assessment Tools and Models

Researchers have captured risk assessment tools and models; however, studies are related to a particular technology group example. The following paragraphs will discuss the risk assessment tools concerned with smart city applications, dimensions, or technology.

Several studies highlight that cybersecurity is a significant risk associated with IoT technology(Lee, 2020; Ande et al., 2020). IoT supports different smart applications in a smart city, including transportation, energy, health, and other dimensions. Accordingly, cybersecurity risk assessment is essential to prevent this risk (Ande et al., 2020; Lee, 2020).

Dimitriadis et al. (2020) developed a cybersecurity risk assessment tool. The authors used a conjunction of OCTAVE and MAGERIT approaches in the proposed tool, proposing a computerized risk estimation in smart sensor environments (AERS). The tool regulates the re-engineering life cycle management process by deploying existing standards and platforms. Attack patterns extract the model for automatically evaluating risks in automated systems.

The authors mention that the proposed assessment tool assists organizations in identifying operating assets within the business process and their related risks.

Accordingly, risk assessment is conducted consistently according to the business needs, which will increase readiness for incident response.

Kandasamy et al. (2020) discussed cybersecurity risk in medical IoT devices and proposed a risk assessment model. The proposed model uses a risk vector for every medical IoT device. Then, the risk rank is provided based on risk impact weight, which will support the management of cybersecurity risks in medical devices.

Security by design for smart city systems was tackled by Ye et al. (2023). This aspect is important in securing connected systems, devices, and applications during the smart city's design phase. The authors introduce a model based on KPI–guided security, called SCKPISec (Smart City KPI-guided Security), that applies unified modeling language (UML) techniques.

The model is tested, and the results proved that the model is highly automated compared to other security models and could efficiently evaluate potential losses in smart city KPIs during threats (Ye et al., 2023).

Ullah (2018) applied three models to construct and evaluate the final risk index: linear approximation, hierarchal fuzzy logic, and a hybrid model based on a combination of both models. The study's result provided that the hybrid model efficiently estimates the final risk index.

The author mentioned that automatic clustering could be performed using the resulting model based on the risk index. The model aims to assist maintenance teams in prioritizing their tasks. Also, the study verified the need for further investigation into advanced risk assessment and estimation methods (Ullah, 2018).

Alawad et al. (2020) investigated smart risk assessment tools in smart mobility, specifically railway applications. The authors introduced an intelligent system for managing risks (ISFMR), a risk assessment model to enhance security and safety within railway applications and to evaluate and control risk efficiently.

The study used an adaptive neuro-fuzzy inference system (ANFIS) as a model to enhance risk management. Artificial neural networks (ANN) train an AI model to expect risks and insecurities based on actual risk information and values. The model improved the accuracy of the risk level projections, learning, and capturing actual-time risk levels. However, the limitation of the study is mentioned as the long time needed for the artificial neural network training and the assumption that the inputs to the risk assessment tool are linear.

Gavurova et al. (2022) proposed a fuzzy risk assessment model to assist decision-makers in managing and establishing required measures in smart cities to provide safe circumstances, including non-pandemics and regular life during pandemics such as COVID-19. The authors tackled different risks of smart city dimensions, including smart security, smart health care, and smart environments. The study mentioned that the suggested fuzzy risk assessment model provides a reasonable risk estimation that supports quality decision-making.

A study by Sharma & Singh (2022) highlighted the usage of AI and machine learning algorithms to advance a smart risk assessment model specifically for cloud computing as a smart city technology. The authors highlighted the need to extensively study security risks in cloud computing, which was not included in their study (Sharma & Singh, 2022). The authors used AI and machine learning algorithms to identify risk factors and predict future risks. The following Table 2.2 summarizes the reviewed models and tools.

Table 2.2. Risk Assessment Tools and Models

Model /Tool	Risk	Smart City Dimension						Author
		Eco	Env	Mob	Gov	Living	People	
cybersecurity risk assessment tool (AERS)	Security	*	*	*	*	*	*	Dimitriadis et al. (2020)
cybersecurity risk in medical IoT devices-Model	Multiple					*		Kandasamy et al. (2020)
Smart City KPI-guided Security	Security	*	*	*	*	*	*	Ye et al., (2023)
Final risk index tool - smart city underground systems	Multiple			*				Ullah (2018)
Intelligent system to manage railway applications in smart city	Multiple			*				Alawad et al. (2020)
Fuzzy risk assessment model for smart cities - health care and environmental systems	Multiple		*				*	Gavurova et al. (2022)
Risk Assessment model for cloud computing as a smart city technology	Multiple	*	*	*	*	*	*	Sharma & Singh, (2022)

2.3 Applications of Management Theories

A smart city strategy is created by the management of an organization.

Therefore, understanding management strategies is essential to design, plan, and implement a smart city (Visvizi & Troisi, 2022). The role of management is usually assessed through applicable management theories by researchers. Also, It is usually mentioned that management emphasizes significant functions related to leading the development, planning, controlling, identifying challenges, analyzing risks, forecasting, sustainable development, and economic growth, considering all smart city dimensions(Schiavone et al., 2020).

Studies have focused on qualitative theories to understand the social factors affecting information technology and infrastructure projects. Different types of qualitative management theories are given(Gioia, 2021; Vanscoy & Evenstad, 2015). Among them, grounded theory and the Gioia method are considered important for large-scale planning. Below is a brief description of the main theories and their applicability in smart city design, planning, implementation, and operation.

Grounded theory is a qualitative research method that considers the complexity of human action and the need to derive knowledge from common conceptual language (Wronowski, 2018). The grounded theory is a mechanism that includes data collection, analysis, explanation, and theoretical combination (Wronowski, 2018). The theory starts from data collection and lets theories develop from the data itself (Glaser et al., 1968).

Grounded theory is used in information technology research to understand human behavior and social factors affecting e-government projects in government organizations (Lee & Kim, 2007). The authors provided that the theory helps to achieve various levels of abstraction related to e-government projects, which are process integration, rewarding systems for employees, training programs, innovative methods to budget information systems, and employees and decision-making beliefs and perception of a project Applying the findings will provide insights to manage IT/IS projects in government sector (Lee & Kim, 2007)

Another related application of grounded theory is given by Techatassaasoontorn & Suo (2010) to explore smart city broadband infrastructure risks. Using the theory, the authors identify risks and conduct a casual mapping analysis to study risk interrelations in broadband government projects. The study proposes five risk categories: social and political, financial, technical, and partnership and resource management risks, and suggests the relations between the five categories identified by applying the grounded theory. The authors mention that risks are interrelated and that management must consider risks from a holistic perspective for better risk management and mitigation. (Techatassaasoontorn & Suo, 2010).

The Gioia method is another method used for management research based on grounded theory. The method focuses on new conception expansion and grounded theory diction. This method supports the initial analysis of scientific theorizing of the research topic (Gioia et al., 2013).

It has been used for data aggregation and analysis to understand the sustainability procedures and their contribution to the logistics sector toward a circular economy (Jayarathna et al., 2022). The authors mention that the Gioia method helped them identify sustainable logistics practices and categorize them into nine categories, which are aggregated into three themes.

Based on Gioia's results, the study concluded that the logistics sector could transfer to the circular economy through environmental preservation, dynamic capabilities, and social well-being (Jayarathna et al, 2022)

Although most of the studies using management research theories focus on non-technical studies, such as understanding social media engagement for pre-teen children

(Lichy et al., 2022) and organizational culture research studies (Gioia, 2000), it is also used to understand future developments and paths at the IT industry (Laato et al., 2022). Managerial decisions affecting agile information system project managers are studied using the GIOIA method by Virag (2021).

The study provides reasons for engaging agile project managers in control activities since the traditional project management style is rarely used in information systems projects. The main reasons are enhancing communication and cooperation, facilitating the association with senior management, and having an overview of other projects (Virag,2021).

Secinaro et al. (2021) used the Gioia method to validate the possibility of using hybrid organization management to manage smart cities. The study benefited from case studies, real natural phenomena, and the Gioia method. The study shows that hybrid theory improves the possibility of directing the output to benefit the smart city's citizens.

Other theories, such as phenomenological theory, are used for management research. The theory centers on the direct examination and explanation of a phenomenon by experienced individuals (Biemel & Spiegelberg, 2024).

The theory is used to study the library and information systems community (VanScoy & Evenstad, 2015). The study provides the effectiveness of the theory in understanding the experience of information specialists and academic library specialists. The authors could identify the details of burnout phenomena and the stages that employees may go through. These stages are the road to burnout, burnout, and life after burnout. Also,the authors provided main recommendations for personal development and organizational enhancements (VanScoy & Evenstad, 2015)

Narrative theory is used in management research since it explores how humans interact with stories and build their meaning. The theory works as a strategy to support elements of peoples' experiences, such as time, process, and support(Summers, 2022). A study by Joseph et al. (2007) used the narrative to understand the reasons for professional turnover in information technology.

The authors mentioned that there are multiple levels affecting IT professional turnover related to the environment, organization, and individual. The study provides a theoretical model built on the results of the narrative method that will support future research on IT turnover(Joseph et al., 2007). Table 2.3 will summarize management theories used in information technology research.

Table 2.3. Management theories used in Information Technology Research

No	Theory	Characteristics	Advantages for Use in This Research	Disadvantages for Use in This Research
1	Grounded Theory	Based on the inductive approach starts with data to reach theory. Precise, structured guidelines. It has a flexible and practical approach to understanding.(Hussein et al., 2014)	A systematic approach to data analysis. Applied for perceptive claims. Depth in collected data. Effective data analysis. (Hussein et al., 2014)	Long process Generalization limits. (Hussein et al., 2014)
2	Gioia method	Based on the inductive approach starts with data to reach the theory. Systematic steps and guideline(Gioia et al., 2013)	Flexible and allows creativity. The method leads to reliable explanations. Scientific rigor. Results in convincing new theories. (Gioia et al., 2013)	Long Process. Time-consuming in data analysis (Gioia et al., 2013).
3	Phenomenological Theory	Based on a philosophical approach. Depends on the experience of people. It creates shared and sometimes competing perceptions. (Leach,2014)	Assets in the development of new theories (VanScoy & Evenstad, 2015) It depends on the experience of people and suits the small scale of research (Leach, 2014)	The subjective approach lacks scientific accuracy. General conclusions cannot be extracted since they are applied on a small scale. (Leach, 2014)
4	Narrative theory	Resolve important stories based on people’s lives. It can be used as a data-gathering method and analytical method. (Ntinda, 2017)	It is easy to convince people to participate since they will tell their stories. In depth data can be	Challenges in understanding the relationship between the old story in data gathering and the story made

No	Theory	Characteristics	Advantages for Use in This Research	Disadvantages for Use in This Research
			gathered(Ntinda, 2017)	in data presentation. Challenges in setting boundaries between stories. (Ntinda, 2017)

The grounded theory supports risk identification and finding risk interrelations (Techatassanasoontorn & Suo 2010). The theory is extensively used to understand the managerial and social aspects of smart cities and risk understanding and categorization for smart city projects. Gioia's method is based on grounded theory and has frequently been used in the last few years to identify management directions for smart cities.

This research study uses the Gioia method, which is based on grounded theory, to analyze the data and explain the risks of smart cities in project phases' design, planning, implementation, and operation. The Gioia method is flexible, allows creativity, leads to reliable explanations, and has scientific rigor that will lead to new theories. Accordingly, it will assist in understanding smart city risks, build connections between collected evidence from different experts to support the quantification process, and lead to the final theory.

2.4 Probabilistic Graphical Models

Managing uncertainties can be achieved using probabilistic graphical models (PGMs). PGMs present a framework based on the probability theory, considering independent relations for a specific challenge. These models lower the complexities of problems under study regarding computational time. The graphs symbolize dependence and independence relations between variables. The joint probability distribution is used in these models to acquire conditional probability. PGMs have several advantages: efficient, easier to communicate and understand, and easy to construct based on experts' knowledge(Spehr, 2015).

Various applications use probabilistic graphical models, including medical diagnosis, engineering, risk assessment, information technology, robotics, and the environment (Spehr, 2015). For instance, PGMs assess economic risks within a project's life cycle. The results showed that using Bayesian Networks, one of the discussed models, can provide qualitative and quantitative information, including dependencies between variables, depending on experts' beliefs (Shishkina, 2015). The main probabilistic models discussed in the following subsections are Bayesian Networks and Markov Networks (Spehr, 2015).

2.4.1 Bayesian Networks

Bayesian network (BN) is a directed acyclic graph where all edges present a specific direction. There should be no cycles within the model. The Bayesian network can be presented in Figure 2.1 (Stephenson, 2000).

The set is represented as E=. $\{(A, B), (A, C)\}$, B and C are considered conditionally independent, then P (B|A, C) = P(B|A), which means that the probability of B is conditioned by A, and the value of the probability of C is unrelated.

Similarly, P (C|A, B) = P(C|A), which means that the probability of C is conditioned by A and the probability of C is unrelated.

Accordingly, the joint probability in this example, as presented by the Bayesian network, can be demonstrated as follows:

P (A, B, C) = P(B|A). P(A).P(C|A). (2.10)

The general equation for the joint probability function in the Bayesian network is presented as follows:

P(X) = $\prod_{i=1}^{n}(P(X_i|Parents\ (X_i))$ (2.11).

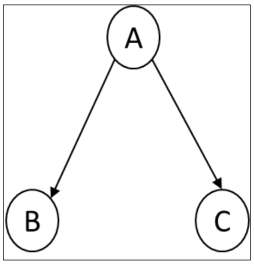


Figure 2.1 Bayesian Network

The joint probability of variables is calculated as each variable's probability, considering the parent’s value using the Bayesian network. In addition, Bayesian network edges are considered causal relations between parent nodes that affect the child node(Stephenson, 2000).

Bayesian networks (BN) have been used in project management to identify risks and challenges (Guinhouya, 2023). Guinhouya, (2023) also mentions that (BN) is used in manufacturing and engineering, construction, IT, and software projects.

BN is used in smart city optimization decisions. For instance, Zhang et al. (2022) combined the naïve Bayesian network with three-way decision-making and filtering algorithms. The suggested model was tested in a smart movie recommendation system and presented better results than two-way decision models. The study provided a model that can be used to promote the construction of smart cities (Zhang et al., 2022). The authors mention that by using this model, the cost is reduced, and the quality is improved of the recommended option(Zhang et al., 2022)

The advantages include its suitability in analyzing uncertainties and calculating joint probabilities. This thesis will use a Bayesian network as a probability graphical model to identify causal relations between smart city risks.

2.4.2 Markov Networks

Markov analysis is used to define the possibility of forthcoming actions given the current condition of a variable. Once the future conditions' probability is determined, a decision tree can be built to calculate the final probability(Beenish et al., 2023),

Markov network is one of the undirected graphical models used to present independent random variables. Edges of the models are undirected; Figure 2.2 presents a Markov network example(Spehr, 2015).

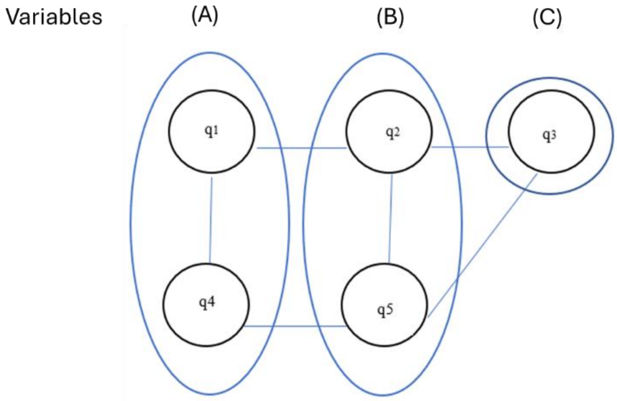


Figure 2.2 Markov Network

Independent variables are defined in the Markov network based on the graph presenting the model. If three variables are presented as (A, B, C), then variable A is independent of variable C given variable B if variable B disconnects A and C in the graph.

Each variable consists of a subset of random variables denoted as “q.” The subset is denoted as a clique. Accordingly, the joint probability distribution for a Markov Network can be calculated using the formula:

P (q1, q2, q3, q4, q5) = (1/Z) P(q1, q4, q5) P(q1, q2, q5)P(q2, q3, q5) (2.12)

Where Z is a normalization factor, Markov probability is applied in this model; the variable is considered independent if all other variables are its neighbors.

The general joint probability formula is denoted as follows:

$$P(X) = \left(\frac{1}{Z}\prod_{c\in Cliques\ (G)} \emptyset\ c\ Xc\ \right) \quad (2.13)$$

Z is a normalizing factor, and ø c is a local function across the variables in the resultant set C (Spehr, 2015).

The Markov Network model is used in diverse fields, such as engineering, medicine, and information technology. It is also used in smart city applications like transportation systems and IoT to estimate transportation density (Beenish et al., 2023)

Beenish et al. (2023) used the Markov Network model as a novel technique for transportation density estimation of a smart transportation system. The research paper showed that the model provided accurate results when estimating traffic density using multiple factors, such as vehicle speed, mean speed, location, and acceleration (Beenish et al., 2023).

In terms of big data analysis, the hidden Markov model is used in smart city networks to solve complexity and uncertainty issues. The model provided a solution even with a minimum amount of data, and reliable results were achieved. Accordingly, smart decisions could be introduced (Prevelianaki & Sherratt, 2023).

In their research, Shanmuganathan & Suresh (2023) combined the Markov model with a long, short-term memory network to detect attacks on IoT devices. Real-time temperature sensors are used to test the proposed models, and results provided effective attack detection with a value of 90% and 94% training accuracy.

Although the Markov Network is used in smart city applications, the main disadvantages of the Markov Network are the requirements of a large number of states, the model is hard to build and validate, and complex systems require a combination of other techniques(Boyd, 1998). Accordingly, the model will not be used in this thesis for risk probability calculations because of the limited number of states of incidents causing risks, but it may be used in risk scenarios' probability calculations.

2.5 Decision Making Techniques

Decision analysis aims to assist the decision-maker in systematic thinking. Where decisions are based on a comprehensive understanding of the problem, this understanding will improve the decision's quality and provide subjective judgments (Clemen & Reilly, 2004).

The decision-making process is constructed from the following steps: problem identification, gathering alternatives, alternatives evaluation, choosing the most suitable alternative, decision implementation, and decision effectiveness evaluation (Danisi et al., 2021).

Accordingly, there are many decision-making tools used to reach a rational decision, such as multidisciplinary tools, decision trees (Shubik, 1958), analytical hierarchy process (AHP) (Clemen & Reilly, 2004), and technique for Order preference by similarity to ideal solution (TOPSIS) The AHP, and TOPSIS will be examined in detail in the following sections.

2.5.1 Analytical Hierarchy Process

The Analytical Hierarchy Process (AHP) is extensively used to process multi-criteria decision-making (MCDM) problems. The core of AHP is based on defining criteria and calculating their weights to assess alternatives.(Russo et al., 2015).

AHP, as a decision-making technique, is performed in several steps that are recognized and used by researchers and summarized in a study by Russo et al. (2015). It is applied in various disciplines, including urban planning and construction of smart cities (Yang & Ma, 2021), business decision-making (Canco et al., 2021), smart city project selection (Wu & Chen, 2021), and Smart city evaluation and ranking (Ye et al., 2022). AHP is used as a decision-making tool in risk assessment studies related to smart cities. For instance, a study by Lyu et al. (2023) reviewed the multicriteria decision-making methods for smart city flood risk assessment. The authors mentioned that incorporating GIS with MCDM will increase the effectiveness of flood risk assessment. To overcome the subjective analysis of MCDM, a fuzzy number is added to better quantitative results (Lyu et al., 2023).

Another study by Bouramdane (2024) used AHP to prioritize and evaluate criteria used for disaster management strategies in smart cities. The authors mentioned that the AHP provided acceptable weights for each management strategy based on the comparison with previous studies.

The main advantages of AHP are its ability to disintegrate the problem into its fundamental elements, and it is easy to use since it allows comparisons between alternatives using a specific criterion in pairs, permitting the identification of relations between alternatives. In addition, it depends on qualitative data, so results are measurable (Zapolskytė et al., 2020). The AHP will be used in this research to evaluate the impacts of risks and calculate the weights of these impacts on smart city sustainability. The risk scenarios will be evaluated based on their impacts.

2.5.2 Technique for Order Preference by Similarity to Ideal Solution (TOPSIS)

The technique for order preference by similarity to ideal solution (TOPSIS) is developed by (Hwang & Yoon, 1981). The approach is designed to select alternatives by calculating the shortest geometric distance from a positive superlative solution and the longest distance from a negative superlative solution. The technique is used in various disciplines, including information technology and smart applications. For instance, it is used to analyze the performance of electronic- supply chain management systems (e-SCM) in the automobile industry. The method is used to evaluate investment alternatives to enhance e-SCM systems. The result supports managers and decision-makers in making robust decisions when setting supply chain strategies (Tyagi et al., 2014). Other studies highlighted using the TOPSIS technique to implement smart waste management strategies. The technique supports decision-makers in deciding successful, reasonable, and appropriate smart waste management strategies(Demircan & Yetilmezsoy, 2023).

Risk assessment is tackled by (Chang, 2015). In his study, the traditional failure mode, effect, and critical analysis (FMECA) are integrated with the TOPSIS technique to solve the challenges of having incomplete data since TOPSIS is suitable for uncertain and incomplete data and situations. The resulting model could handle decision-making problems effectively (Chang, 2015). The TOPSIS technique is reviewed in case the research faces an incomplete set of data.

In summary, this chapter reviews the literature, considering risk assessment tools and methods and concentrating on the methods used in smart city research. Also, applications of management theories in engineering research, probabilistic graphical models, and their usage in different disciplines, including smart applications studies, are examined. Then, the decision-making techniques, namely, multiple criteria decision-making techniques, are explored.

2.6 Literature Review Summary and Gaps

The literature review shows different models for specific risk assessments, and they are applied in different contexts, often focusing on a particular application situation. As per Alawad et al. (2020), there are limited risk assessment models that consider a comprehensive view of smart city design, planning, implementation, and operation. The review further shows that there are opportunities to analyze the risks perspectives from the managerial point of view by considering the total design, plan, implementation, and operation of smart cities.

Although comprehensive risk assessment is necessary, there is a lack of research on the risk assessment tools and the assessment frameworks that help to analyze the impact of risks in different aspects of smart city development. Without such a tool, it is difficult to understand the integrated impact of risks in smart cities. Therefore, the research can be extended to develop a comprehensive and flexible framework by using risk assessment tools. The framework should be valid for use during any phase of smart city development and operation.

The smart city is also a social system, and the decision-making to integrate different services and technology is also based on the given decision-making environment. This requires thorough management research so the experts' perceptions can be compiled for designing, planning, implementing, and operating smart cities. Therefore, the second research direction is to focus on management research based on grounded theory for understanding smart city risks, their probabilities of occurrence, and their impacts. Therefore, in this research, a comprehensive risk assessment tool is proposed. The tool's utility for risk assessment is verified and validated through a comprehensive directed study of smart city design, planning, implementation, and operation processes. The second aspect of the research is to develop a grounded theory on risk based on management research by using the Gioia method to analyze the data and explain the risks of smart city design, planning, implementation, and operation.

The thesis adopts the Gioia method due to the systematic approach it utilizes to elicit and analyze data. The tool and the management approach are integrated to propose a holistic smart city risk assessment framework, which will be discussed in the next chapter.

CHAPTER 3: RESEARCH METHODOLOGY

The research methodology adopted in this research uses the design research science paradigm, which combines behavioral science and design science. Behavioral science relates to the understanding of human and organizational behavior in a case (Hevner & Chatterjee, 2010). Design science relates to scientific patterns used by scientists to solve a scientific problem. (Van Aken, 2004)

Design research science is used to create innovative frameworks, artifacts, or systems to find solutions to a specific case (Adikari et al., 2009). This paradigm is widely used in engineering disciplines (Hevner & Chatterjee, 2010).

The details of the research methodology are discussed in the following sections.

3.1 Sampling Strategy

A purposive and convenient sample is used in this research to seek information for the development of a risk assessment model. A purposive sample is a sample where the researcher selects subjects that only satisfy the objectives of the research based on the researcher's belief. A convenient sample is a sample obtained from a population that is available and accessible to the researcher (Isaac, 2023).

Purposive sampling is used in research related to many disciplines (López, 2022). The usage of this sampling method for engineering-related research is supported by a study by Smith et al. (2013). The author used the sampling method to determine the main system engineering processes in high-development projects. The purposive sample is recognized as an efficient, consistent, and unbiased sample (López, 2022).

Also, a convenient sample presented reliable results as per a study by Escorcia-Guzman et al. (2021). The author used a convenient sampling method to study information technology distribution and its usage in higher education organizations.

Accordingly, the used sample for the research is considered purposive since the interviewed candidates are smart city experts who are involved in the design, planning, implementation, or operation of the smart city, use and manage smart applications, manage information technology department within a smart city, support or operate smart applications, or has a strategic or high management role within a smart city. Also, the sample is convenient because the experts are accessible through work connections. Forty experts are interviewed, the researcher has a direct work relationship with ten of these experts, and the remaining thirty candidates are reached out through snowballing, where research participation is recommended by the first ten candidates to their connections.

3.2 Proposed Holistic Smart City Risk Assessment Framework.

Based on the discussion in earlier chapters, a risk assessment framework developed based on the BLOC-ICE concept is proposed in Figure 3.1. The BLOC-ICE concept is proposed by Pokharel (2023) and helps to visualize, explore, and elaborate the risk assessment. The approach is used to study problems and opportunities in different fields, including technical, business, and social systems (Pokharel, 2023). The description of the framework is given in the sections below, for the framework inputs are obtained from the interviews with the stakeholders.

The proposed framework is structured in three phases: Phase 1—initial data analysis; Phase 2—calculation of the basic probability assignment and incidents classification and interrelations; and Phase 3—identification and evaluation of risk scenarios. Each phase produces an outcome that contributes to the suggested risk assessment model. Each phase is described in detail in the following sections.

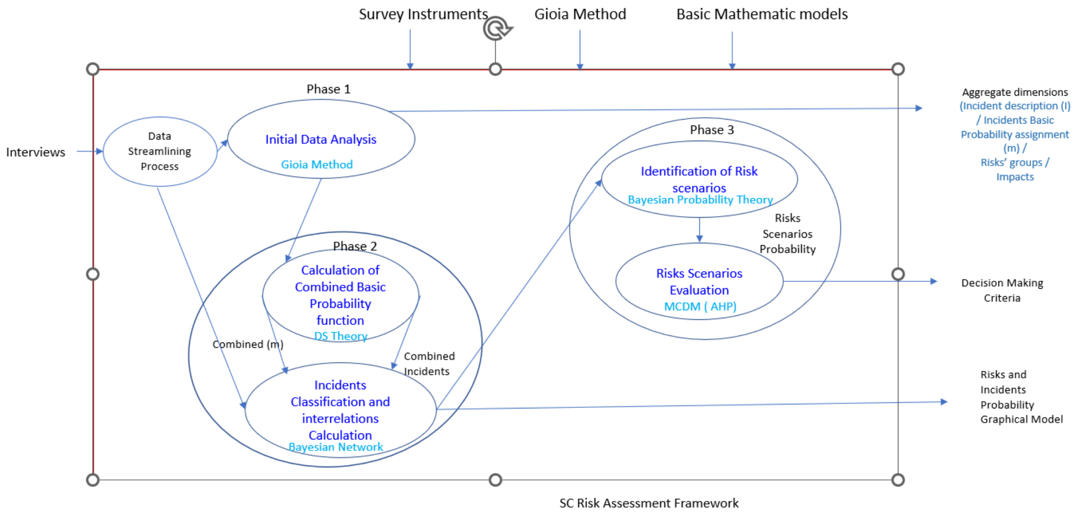

Survey Instruments
Gioia Method
Basic Mathematic models
Interviews
Data Streamlining Process
Phase 1
Initial Data Analysis
Gioia Method
Phase 2
Calculation of Combined Basic Probability function
DS Theory
Combined (m)
Combined Incidents
Incidents Classification and interrelations Calculation
Bayesian Network
Phase 3
Identification of Risk scenarios
Bayesian Probability Theory
Risks Scenarios Probability
Risks Scenarios Evaluation
MCDM (AHP)
Aggregate dimensions
(Incident description (I) / Incidents Basic Probability assignment (m) / Risks' groups / Impacts
Decision Making Criteria
Risks and Incidents Probability Graphical Model
SC Risk Assessment Framework

Figure 3.1: Risk Assessment framework for smart city

3.2.1 Data streamlining

Data is collected through interviews with open-ended questions to initiate the discussion. The resulting data is processed and streamlined for analysis. The data streamlining includes writing interview scripts, assigning the ranks to risks and risk incidents gathered from the interviews, and performing statistical analysis, including the Cronbach reliability test and Pearson Correlation test for the gathered data.

3.2.2 Phase 1: Initial Data Analysis

Initial data analysis is based on the grounded theory approach, and as discussed earlier, the Gioia method is used for this analysis. The use of the method for initial data analysis is also recommended by Corbin & Strauss (1990) and Secinaro et al. (2021). For this purpose, interviews are conducted, the scripts are studied and coded, and data analysis is performed to understand the incidents causing the risks. Open coding is applied to experts' descriptions of the implemented applications in a smart city and the main challenges faced during designing and planning, implementation, and operation.

Open coding generates the first-order codes. The mentioned challenges are coded as incidents (I) that may cause risks. Then, the risks that may occur during the planning, implementation, and operation are defined and coded to develop the second-order themes. The method also involves basic probability assignment coded as (m) of a specified incident causing a risk. Axial coding, which is the process of relating defined categories to the sub-categories, is used to relate different risks to the defined incidents (I).

Second-order themes are created based on the Gioia method (Gioia et al., 2013). The second-order themes are the risks of specific incidents (I). Then, the third-order themes are defined through further consolidation of the second-order theme. The consolidation of the grounded theory is based on analyzing the scripts and discussions with each participant. The method allowed data analysis and consolidation until the aggregated dimension was reached (Gioia et al., 2013).

The method is applied based on the above theoretical explanation in this research, which is as follows: The resulting scripts from the interviews are analyzed line by line, keywords related to smart city challenges and threats are highlighted and coded using open coding as incidents causing risks (*I*). The participants are asked to rank the chance of occurrence for each threat or challenge, and these ranks are coded as the basic probability assignments for incidents (*m*). The incidents causing risks (*I*) and the ranks incidents' basic probability assignments (*m*) represent the first-order theme. From the discussions with experts, the most common incidents causing a specific risk have been identified. Accordingly, the risks are linked to the incidents that caused them, and the second-order theme resulted. Also, inspecting the scripts, the different risks were related to specific phases of the smart city project: design, planning, implementation, and operation. The risks that may occur within a specific project phase are aggregated, forming the third-order theme, which presents project phase risk. The impacts of risks on smart city projects and smart city sustainability are highlighted and linked to the smart city project phase. Therefore, the aggregated dimension presents the impacts and their links to the project phase risk, which is defined per the experts' observation as a major impact at this specific phase, and then grounded theory results. The results of this phase are shown in section 4.4.1.

The incidents causing risks (I) and the ranks of incidents' basic probability assignments (m), which are the first-order themes, will be used to calculate combined probability assignments for each risk using the Dempster – Shafer theory in the second phase of the framework.

3.2.3 Phase 2: Combined (m) Calculation and Risks' Interactions

In this phase, the risk assessment tool in the proposed framework in Figure 3.1 is developed by combining the Dempster-Shafer theory with the Bayesian theory to provide a rich understanding of risks and uncertainties.

The Dempster-Shafer theory is used to get the combined basic probability assignment (m_{12}) for incidents causing each risk. Resulted from the initial data analysis, phase 1 of the framework.

The basic probability assignment (m) is envisioned by evidence theory. The theory has three main functions: the basic probability assignment function (m), the Belief function (*Bel*), and the Plausibility function (*Pl*). The basic probability function distinguishes the function of the power set for the interval from 0 to 1 equation (3.1), and m ($\emptyset$) is zero, equation (3.2), and the total of (m) for all subsets of the power set is

1 equation (3.3)

Suppose the definition is applied for a set A; for instance, the basic probability assignment for a set A is represented as m(A) and formulates the fraction of related indication to support the assumption that a specific element of X (universal set) belongs to set A. Another basic belief function, m, will represent more evidence in the subset (Sentz and Ferson 2002). Then, the presentation of basic probability is as follows:

$$m: P(X) \rightarrow [0,1] \tag{3.1}$$

$$m(\emptyset) = 0 \tag{3.2}$$

$$\sum_{A \in P(X)} m(A) = 1 \tag{3.3}$$

P(X) is the power of set X and $\emptyset$ the null set.

The interval (0,1) is constrained by two determines: the belief and the plausibility. The belief function of set A: *Bel*(A) is the sum of all basic probability assignments (*m*) of a subset (B) of set A.

The plausibility: Pl(A) is the sum of the basic probability assignments of a set (B) that intersects with set A (Sentz and Ferson 2002).

$$Bel(A) = \sum_{B|B \subseteq A} m(B) \tag{3.4}$$

$$Pl(A) = \sum_{B|B \cap A \neq \emptyset} m(B) \tag{3.5}$$

The values of the belief function and plausibility are nonadditive. Accordingly, the sum of all belief measures is not required to be 1, and the same applies to plausibility measures (Sentz and Ferson 2002). Additionally, the two functions can be derived from each other as follows:

$$Pl(A) = 1 - Bel(\neg A) \tag{3.6}$$

Where $(\neg A)$ (note A) complements A, this definition comes from the sum of basic probability assignments as 1.

Aggregating multiple basic probability assignments (m) based on experts' knowledge and experience of risk incidents is achieved using the Dempster-Shafer combination rule. This rule strongly emphasizes the agreement of different sources and overlooks conflicting evidence using a normalization factor.

The combination rule symbolizes a strict AND operation (Sentz & Ferson, 2002). Joint basic probability assignment (m_{12}) is calculated by summing the products of basic probability assignments of all sets (incidents in this study), as equation (3.7). The combined basic probability assignment m_{12} of the null set is (0) equation (3.8). K is the basic probability assignment of a conflict situation when the intersection between the incidents is a null equation (3.9). 1-K is the normalization factor used to ignore the effect of conflict.

Table 3.1: Dempster Shafer Combination Rule Parameters

Notation	Description
m_{12} (A)	Combined basic probability assignment of a set of interest (A)
m_1 (B)	Basic probability assignment of a subset (B)
m_2 (C)	Basic probability assignment of a subset (C)
K	Basic probability assignment of a conflict situations

The following formulas illustrate the combination rule. The rule combines the basic probability assignment of a subset (B), in the case of this research, is risk's incident (1), with the basic probability assignment of a subset (C), Incidents (2), where A is the set of incidents causing this specific risk.

$$m_{12}\,(A) = \frac{\sum_{B\cap C=A} m_{\,1}\,(B)\, m_2\,(C)}{1-K}, \text{ when } A \neq \emptyset \quad (3.7)$$

$$m_{12}\,(\emptyset) = 0 \qquad (3.8)$$

Where:

$$\text{K} = \sum_{B\cap C=\emptyset} m_1\;(B) m_2\,(C) \quad (3.9)$$

Using the above theory and equations on the resulting data from phase 1 is performed as follows :

- The incidents causing risks (I) and the ranks of incidents (are tabulated for each risk, where incidents are mentioned, and the rank given by each expert is provided.
- The basic probability assignment is calculated by dividing the number of experts ranked in the incident with rank R by the total number of experts mentioned in this incident.
- The incident will have multiple basic probability assignments based on experts' ranking. For instance, incident one will have a basic probability assignment. m_1 based on experts ranking it high, m_2 based on experts ranking it low.
- Each risk is caused by multiple incidents, and the incidents' basic probability assignments are calculated.
- Using the Dempster- Shafer combination rule equation (3.7), the combined basic probability assignments m_{12} for incidents causing each risk are generated, results are illustrated in section 4.4.2
- The resulting combinations are used to calculate the probability of risk to occur using Bayesian theory and to identify the interrelations using Bayesian Network (BN) as discussed in the following paragraph.

Bayesian network (BN) is a probabilistic graphical model, as discussed in 2.4.1.BN is used to show incident relations to a specific risk graphically and to present various risk interrelations derived from expert interviews and the analysis of the common incidents between risks. Resulted from the initial data analysis phase.

Bayesian network edges are causal relations between parent nodes that affect the child node (Stephenson, 2000). All the edges in the graph present a specific direction. Figure 3.2 presents the Bayesian network. The scenarios of risk interrelations are graphically presented in section 4.4.2.

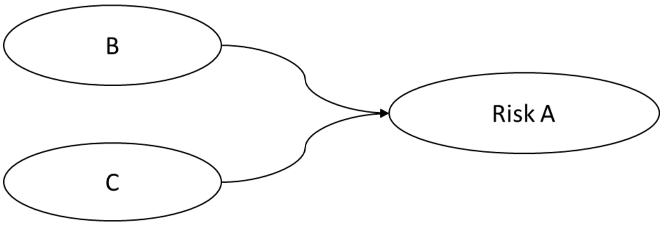


Figure 3.2 Bayesian Network Application at The Research Data

Based on the graphical presentation of BN, for each relation, the set of edges of the Bayesian network is represented as E= {(A, B) (A, C) }, B and C are considered conditionally independent, then P(A|B, C) = P(A|B), which means that the probability of risk A to occur is conditioned by the value of the probability of combined incidents B occurrence and the value of the probability of combined incidents C is unrelated. Similarly, P (A| C, B) = P(A|C), which means that the probability of risk A to occur is conditioned by combined incidents C occurrence and the probability of combined incidents B is unrelated.

Based on the above discussion, the probability of risk A to occur due to combined incidents B and combined incidents C can be calculated using Bayes theory as follows:

- Let U be the event that risk A occurs due to combined incidents B and combined incidents C, i.e., U = B ∩ C. Using Bayes' theorem, we have:

$$P(\mathrm{A}|\mathrm{U}) = \frac{\mathrm{P}(\mathrm{U}|\mathrm{A})\mathrm{P}(\mathrm{A})}{\mathrm{P}(\mathrm{U})} \tag{3.10}$$

P(U|A) is the probability of risk A risk due to the combined incidents B and C, and P(U) is the marginal probability of risk A considering both combined incidents occur.

- To calculate P(U|A), we can use B and C as independent events given A.

  $$\mathrm{P(U|A)} = \mathrm{P(B|A)\ P(C|A)} \tag{3.11}$$

- To calculate P(U), we can use the law of total probability and the fact that A and ¬A are separate events, according to the below formula:

  $$\mathrm{P(U)}=\mathrm{P(U|A)\ P(A)}+\mathrm{P(U|\neg A)\ P(\neg A)} \tag{3.12}$$

  P(U|¬A) is the probability of combined incidents B and C to happen, given that risk A does not occur, and P(¬A) is the probability of risk A not occurring.

- Given that B and C are independent events given ¬A, the formula below is used to calculate. P(U|¬A).

  $$\mathrm{P(U|\neg A)} = \mathrm{P(B|\neg A)\ P(C|\neg A)} \tag{3.13}$$

- P(U) is calculated using the formula (3.12), then the P(A|U) is calculated using the formula (3.10).

The mentioned mechanism is used to calculate risk probabilities caused by combined incidents.

Bayesian network (BN) is suitable for analyzing uncertainties and calculating joint risk probabilities in this study. The result of this phase is a graphical representation of the risks based on the experts' interviews and analysis of the common incidents between risks. Risk probabilities are calculated using the Bayes theorem.

The relationship between different identified risks is presented following Bayesian network characteristics that will lead to risk scenarios. Identifying scenarios is essential to guide the analysis towards the targeted decision-making criteria. Accordingly, the probability of each scenario is quantified using Bayesian joint probability in phase 3 of the framework.

3.2.4 Phase 3: Risk Scenarios Identification and Evaluation

In this phase, risk scenarios are defined using the graphical model. Bayesian probability theory is applied to calculate the joint probability for each scenario. The theory will be applied to the combined basic probability assignment for a risk. Accordingly, the joint probability resulted from other risks causing risk (A), for instance, is demonstrated as:

$$P\ (A, B, C) = P(B|A).\ P(A).P(C|A). \qquad (3.14)$$

The general equation for the joint probability function in the Bayesian network is presented as follows:

$$P(X) = \prod_{i=1}^{n}(P(X_i|Parents\ (X_i)) \qquad (3.15)$$

Stephenson (2000), in his study introducing and using Bayesian theory, provides that the joint probability of variables under study is the probability of each variable, considering the parent’s value. In addition, Bayesian network edges are considered interrelations between parent nodes that affect the child node (Stephenson, 2000). The following steps illustrate how this theory is applied to reach outcomes.

- The graphical presentation of an identified risk scenario based on the outputs of phase 1, where common incidents of risks are highlighted and relations are mentioned by smart city experts, are illustrated.
- The probability of the parent risk to occur due to its incidents is calculated using

the Bayes theorem equation (3.10).

- The probability of the risk scenario is calculated using the Bayesian network joint probability equation (3.15). The results of this phase are presented in 4.4.3

The resulting joint probability for each risk scenario is used to reach the decision-making criteria by evaluating the risk scenarios against the impacts on smart city sustainability using the Analytical Hierarchy Process (AHP). The process is used to explain multi-criteria decision-making (MCDM) problems.

The technique will be applied by structuring the problem hierarchy and identifying the evaluation criteria. The evaluation criteria are the impact of the smart city project on the main defined aspects: service continuity, service efficiency, resource productivity, smart city reputation, and revenue generation. Concerning each criterion, mathematically, risk scenarios will be ranked; then, the ranks will be combined to set a score for each scenario. Decision-making criteria are developed based on the resulting scores of risk scenarios.

The process of AHP is described as follows:

- Problem definition and goal determination.
- Hierarchy structuring the hierarchy from high-level objectives to low-level alternatives.
- Pair-wise comparison matrices (size $n \times n$) are constructed, where one matrix is for each element in the level.
- The pair-wise comparisons are determined by the preference of one element over the other using a scale from 1 to 9 introduced by (Saaty, 1987). One is given when both criteria have the same significance. This matrix is denoted as A1.
- The relative normalized weight (W_j) is found for each criterion by normalizing

the mean of rows in the comparison matrix(Saaty, 2013).

- The consistency is verified by using the eigenvalue of a matrix γ_{max} , by calculating the consistency index CI where
- $CI = \frac{\gamma_{max} - n}{n-1}$ (3.16)

n is the matrix size.

- Concluded evaluation matrix consistency can be checked by calculating the consistency ratio CR for matrix size. If CR≤ 0.1, the concluded evaluation matrix is accepted.(Awasthi & Chauhan, 2011).
- An evaluation vector is used in evaluating each risk scenario using the weighted sum method. If there are *m* alternatives and *n* criteria, the suitable alternative is the one that satisfies the equation (Mateo, 2012).

$$A^{*}_{wsm} = \text{Max} \sum_{i}^{j} a_{ij} \ w_j \qquad (3.17)$$

For i =1,2, … *m* Where A^{*}_{wsm} is the score resulting from the weighted sum method. The number of decision criteria is denoted by *n*, a_{ij} represents the actual value of the *i* th alternative about the *j* th criterion and w_j Represents the weight of importance of the *j*th criterion. The following steps are followed to use the theory :

- The hierarchy is constructed, where the goal is to reach smart city sustainability. The second level presents the impacts on smart city sustainability. The third level is the smart city project phase risk, and the lower level is the risk scenarios.
- The impacts of risks are extracted from the data and analyzed using the Gioia method.
- The ranks of the impacts in comparison to each other are derived based on the experts' views.
- AHP steps are applied to derive the pair-wise comparison matrix for the impacts

and get the weight for each impact.

- The ranks of risks based on the project phase are generated based on the initial beliefs of experts.
- AHP steps are applied to derive the pair-wise comparison matrix for each of the smart city projects and compare them with each impact. Accordingly, The weights are derived.
- The final decision matrix is constructed using the results from the previous steps.

For this study, the highest value presents a risk scenario with the highest probability and impact on smart city projects. The results are presented in section 4.4.3

3.3 Validation of the Framework

Focus group with candidates from two smart city projects in Qatar are targeted to validate and evaluate the model. The first project is in the operation phase, and the second is in the implementation phase. Fifteen candidates participated in the focus group meeting. During the focus group, the outcome of each phase of the smart city risk assessment framework is explained and discussed. Participants are requested to evaluate the outcomes of each framework phase using. The system usability scale (SUS) (Brooke, 2020). The evaluation was sent to the candidates after the meeting, and responses were received in a week’s time. The evaluation results are provided in section 4.5

3.4 Chapter Summary

In this chapter, the smart city risk assessment framework is presented. The suggested framework will identify incidents causing risks using the Gioia method from expert interviews. The identified incidents and related risks will be checked and compared with those mentioned in the literature. Experts’ beliefs about the occurrence of each incident will be used to calculate combined basic probability assignments for each risk. The interview data will be used to derive risk interrelations and presented using a Bayesian network as a graphical probability model. Bayesian theory will calculate joint probability for each scenario, and then, scenarios will be evaluated using the analytical hierarchy process.

CHAPTER 4: DATA ANALYSIS AND RESULTS

This chapter will present the results from the analysis of the proposed research framework. The results for each framework phase are shown and described in detail.

4.1 Data Collection

The targeted sample is seventy-five smart city experts. The sample is purposive and convenient since the first ten candidates satisfy the research objective and are accessible to the researcher. Snowball sampling is used after the initial sample is drawn. The sampling technique is non-random and empirical, depending on networking to identify obscure populations (Dragan & Isaic, 2022). For the interviews, respective smart city experts are targeted, including strategic planners, decision-makers, application designers, analysts, enterprise architects, IT directors, and smart application users.

Interviews are scheduled with experts in face-to-face setup or MS Teams ®. The interviews are designed as semi-structured and open-ended Interview questions available at (APPENDIX A) started with identifying the smart applications used in the smart city, the risks associated with these systems, their classification as technology or non-technology risks, incidents causing such risks, and their impact on smart city implementation and operation. Detailed notes were taken to allow analysis in the following steps.

The interviewing process was stopped after interviewing 40 experts since the respondents identified no new risk. Table 4.1 demonstrates the responses of experts, arranged based on the interview sequence and the risks mentioned. It is seen that the replication of the identified risks started after the results of interviews obtained from Expert 12. Accordingly, saturation points of the data resulted. Hennink and Kaiser

(2022) also mention this type of saturation level. The authors mentioned that the saturation level for the inductive research approach is between 9 and 17 interviews, especially when the sample is homogeneous.

Based on their role in smart city design, implementation, and operation, the interviewees are categorized into four categories: smart city strategic planners, smart city implementers, smart city operators, and smart city application users. The percentage of smart city planners in relation to the total number of participants is 15%; smart city implementers create 57.5% of the sample, smart city operators are 15% of the sample, and smart city application users are 12.5% of the sample. Table 4.2 below will present the groups of experts and their years of experience, ranging from 3 years to 30 years, and their job titles within the smart city project.

Table 4.1. Candidates Profiles and Mentioned Risks

Expert	Expert Profile	Category	Cyber-security Risk	Technical Data and Application Risk	Data Security and Privacy Risk	Integration Risk	Strategic Risk	Stakeholders' Engagement Risk	Business continuity	Resources, resource management, Risk	Financial Risk	Laws, regulations, and Standards Risk	Network Infrastructure Risk
1	Senior Enterprise Application Architect	SC Implementers	*	*	*	*	*	*	*				
2	IT Director	Smart Application User	*	*			*						
3	IT Director	Smart Application User	*							*			
4	Head of IT	Smart Application User			*					*			

Expert	Expert Profile	Category	Cyber-security Risk	Technical Data and Application Risk	Data Security and Privacy Risk	Integration Risk	Strategic Risk	Stakeholders' Engagement Risk	Business continuity	Resources, resource management, Risk	Financial Risk	Laws, regulations, and Standards Risk	Network Infrastructure Risk
5	Smart City Rollout Project Manager	SC Implementers				*	*	*		*			
6	Research and Development Engineer	SC Implementers	*							*			
7	Senior Client Service Architect	SC Implementers	*	*			*						
8	Managing Director	SC Strategic Planners	*	*	*		*	*		*	*	*	
9	Chairman - CEO	SC Implementers	*	*								*	

Expert	Expert Profile	Category	Cyber-security Risk	Technical Data and Application Risk	Data Security and Privacy Risk	Integration Risk	Strategic Risk	Stakeholders' Engagement Risk	Business continuity	Resources, resource management, Risk	Financial Risk	Laws, regulations, and Standards Risk	Network Infrastructure Risk
10	Smart Platform Channel Lead	SC Implementers										*	
11	Program Manager	SC Operators					*				*		
12	ICT Operation Manager	SC Operator s	*			*							*
13	Senior Smart Campus Integration Specialist	SC Strategic Planners					*	*		*	*		
14	Chairman - CEO	SC Strategic Planners	*		*	*			*	*			*
15	Lead Support Engineer	SC Operators		*		*		*	*			*	

Expert	Expert Profile	Category	Cyber-security Risk	Technical Data and Application Risk	Data Security and Privacy Risk	Integration Risk	Strategic Risk	Stakeholders’ Engagement Risk	Business continuity	Resources, resource management, Risk	Financial Risk	Laws, regulations, and Standards Risk	Network Infrastructure Risk
16	Applications Consultant	SC Implementers	*	*	*		*	*		*			
17	SC Consultant	SC Implementers						*			*		
18	Smart City Expert	SC Implementers	*				*	*				*	
19	Regional Service Provider Director	SC Implementers	*				*		*	*	*	*	
20	CEO-Founder	SC Implementers	*			*		*	*	*	*	*	
21	SC Consultant	SC Implementers	*	*	*	*	*	*		*		*	*

Expert	Expert Profile	Category	Cyber-security Risk	Technical Data and Application Risk	Data Security and Privacy Risk	Integration Risk	Strategic Risk	Stakeholders' Engagement Risk	Business continuity	Resources, resource management, Risk	Financial Risk	Laws, regulations, and Standards Risk	Network Infrastructure Risk
22	SC Consultant	SC Strategic Planners					*	*	*	*			
23	Risk and Compliance Consultant	SC Strategic Planners					*	*		*	*	*	*
24	Chairman - CEO	SC Implementers	*			*				*		*	
25	Project Manager	SC Implementers	*							*		*	*
26	Service Delivery Manager	SC Implementers		*	*			*		*		*	
27	Project Manager	SC Implementers	*				*						

Expert	Expert Profile	Category	Cyber-security Risk	Technical Data and Application Risk	Data Security and Privacy Risk	Integration Risk	Strategic Risk	Stakeholders’ Engagement Risk	Business continuity	Resources, resource management, Risk	Financial Risk	Laws, regulations, and Standards Risk	Network Infrastructure Risk
28	Digital Transformation Expert	SC Implementers					*	*	*	*	*	*	
29	Smart City Expert	SC Implementers		*			*	*	*				*
30	Managing Director	SC Implementers	*		*	*		*		*		*	
31	ICT Engineer SC	SC Operators	*	*			*	*		*			
32	Project Manager	SC Implementers			*	*	*	*		*	*	*	*
33	Lead Cybersecurity Engineer	SC Implementers	*		*	*				*		*	

Expert	Expert Profile	Category	Cyber-security Risk	Technical Data and Application Risk	Data Security and Privacy Risk	Integration Risk	Strategic Risk	Stakeholders' Engagement Risk	Business continuity	Resources, resource management, Risk	Financial Risk	Laws, regulations, and Standards Risk	Network Infrastructure Risk
34	Senior Program Manager	SC Implementers	*		*	*		*		*		*	*
35	Cluster IT Director	Smart Application User	*				*			*	*	*	*
36	Cyber Security Engineer	SC Implementers			*	*						*	
37	Cluster IT Director	Smart Application User	*		*		*	*	*	*	*	*	
38	SC IT Director	SC Operators	*		*	*	*			*	*	*	
39	SC security Engineer	SC Operators	*		*	*	*	*		*	*	*	*

Expert	Expert Profile	Category	Cyber-security Risk	Technical Data and Application Risk	Data Security and Privacy Risk	Integration Risk	Strategic Risk	Stakeholders’ Engagement Risk	Business continuity	Resources, resource management, Risk	Financial Risk	Laws, regulations, and Standards Risk	Network Infrastructure Risk
40	Digital Transformation Expert	SC Strategic Planners	*		*	*	*	*	*	*	*	*	

Table 4.2 Categories of Candidates and Percentage in Relation to the Sample

No	Category	Job Title	Years of Experience	Number of Experts	Percentage
E5	SC Implementers	Smart City Rollout Project Manager	25	23	0.575
E1		Senior Enterprise Application Architect	17		
E6		Research and Development Engineer	3		
E7		Senior Client Service Architect	25		
E9		Chairman - CEO	35		
E10		Smart Platform Channel Lead	15		
E16		Applications Consultant	30		

No	Category	Job Title	Years of Experience	Number of Experts	Percentage
E17		SC Consultant	30		
E18		Smart City Expert	30		
E19		Regional Service Provider Director	30		
E20		CEO-Founder	20		
E21		SC Consultant	26		
E24		Chairman - CEO	20		
E25		Project Manager	10		
E26		Service Delivery Manager	23		
E27		Project Manager	20		
E28		Digital Transformation Expert	20		
E29		Smart City Expert	20		
E30		Managing Director Cybersecurity	25		
E32		Project Manager	18		
E33		Lead Cybersecurity Engineer	5		
E34		Senior Program Manager	23		
E36		Cyber Security Engineer	5		

No	Category	Job Title	Years of Experience	Number of Experts	Percentage
E11	SC Operators	Program Manager	35	6	0.15
E12		ICT Operation Mananer	25		
E15		Lead Support Engineer	25		
E31		ICT Engineer SC	15		
E38		SC IT Director	25		
E39		SC Security Engineer	15		
E8	SC Strategic Planners	Managing Director	30	6	0.15
E13		Senior Smart Campus Integration Specialist	28		
E14		Chairman - CEO	28		
E22		SC Consultant	26		
E23		Risk and Compliance Manager	30		
E40		Digital Transformation Expert	25		
E2	Smart Application User	IT Director	20	5	0.125
E3		IT Director	26		
E4		Head of IT	17		
E35		Cluster IT Director	25		

No	Category	Job Title	Years of Experience	Number of Experts	Percentage
E37		Cluster IT Director	25		

4.2 Time Frame of Research Work

The interviews are conducted over six months. Due to the FIFA World Cup 2022 organization in Qatar, many local experts expressed their unavailability before, during, and after the tournament. Yet the interviews took place through MS Teams, after the tournament.

4.3 Data Reliability

The reliability of the collected data is tested using the Cronbach alpha (Cronbach, 1951) test, which is widely used for reliability tests of data (Schweizer et al., 2015). In this thesis, the test is performed using SPSS® Software. Table 4.3 shows the reliability factors for different sample sizes(Bujang et al., 2018). The analysis of the collected data shows that for a response size of 40, the Cronbach Alpha value is 0.852. Therefore, based on the table, the data obtained is considered reliable.

Table 4.3. Cronbach Alpha for Different Sample Sizes

Sample Size (n)	Cronbach Alpha
130	0.65
64	0.7
36	0.75
22	0.8
14	0.85

4.4 The Smart City Risk Assessment Framework Results

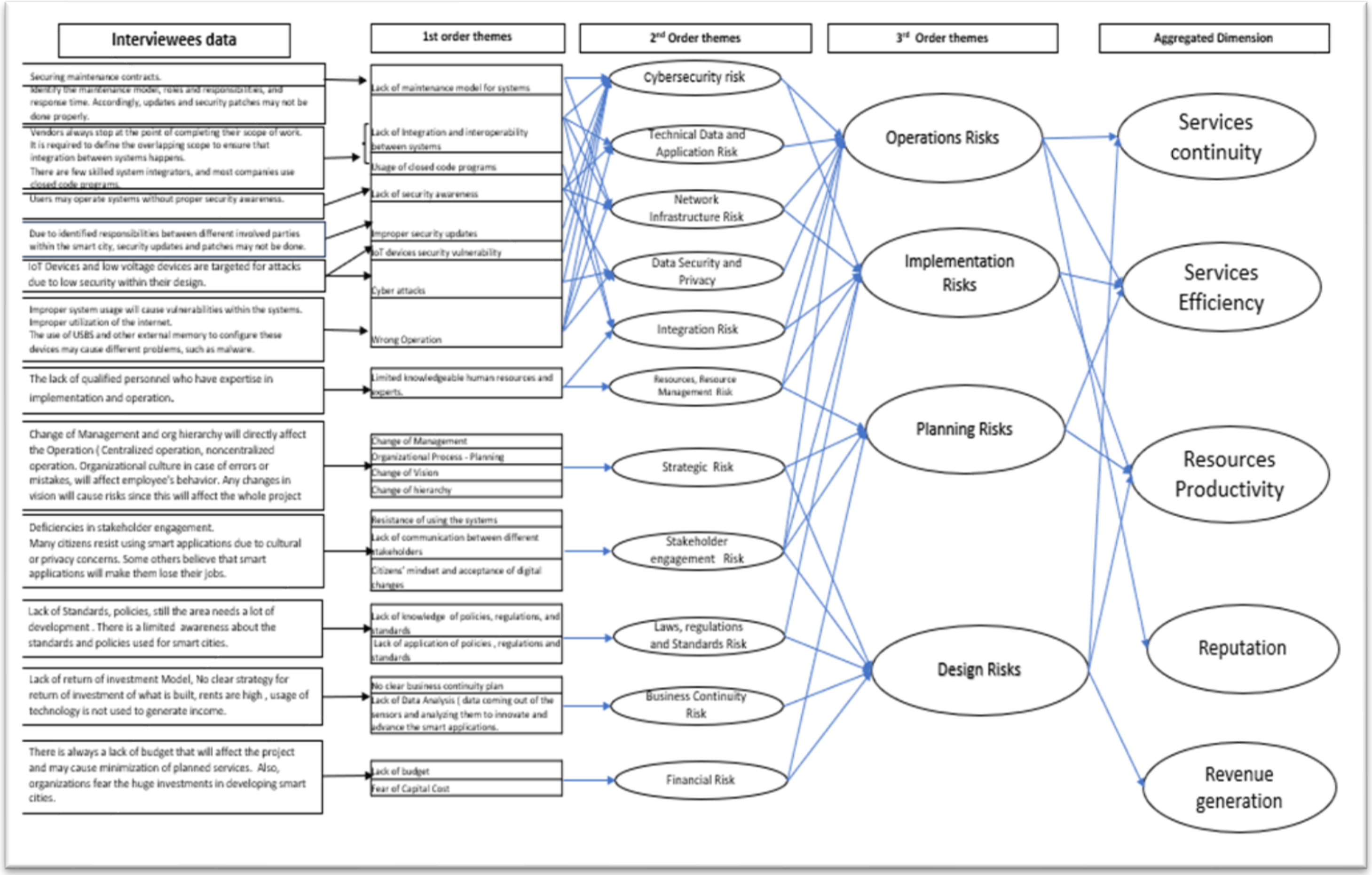
4.4.1 Phase1: Initial Data Analysis

This section gives the results of Phase 1 from the suggested framework in Figure 3.1. Using the Gioia method, interview responses are analyzed and transcribed to elicit the challenges related to smart city design, planning, implementation, and operation.

Threats and incidents causing risks during the smart city project and organizational factors affecting planning, implementation, and operation are also defined. The interrelations between identified risks and business impacts are specified, in addition to the rank of each incident to occur. Then, the second-order themes are derived from incidents causing risks, and the basic probability assignment for each incident is determined to be used to identify the probability of each of the risks faced in the smart city project.

The risks are regrouped based on their effect to construct the third-order themes. The third-order themes are four risk groups: design risks, planning risks, implementation risks, and operation risks.

The aggregated dimension represents the impacts of these groups on smart city sustainability; these impacts are related to smart city service continuity, service efficiency, resource productivity, reputation, and revenue generation. The detailed steps of the mechanism used to achieve the outcomes of this phase are mentioned in section 3.2.2. The results of the Gioia method are illustrated in Figure 4.1 and described in the following paragraphs



Securing maintenance contracts.
Identify the maintenance model, roles and responsibilities, and response time. Accordingly, updates and security patches may not be done properly.

Vendors always stop at the point of completing their scope of work.
It is required to define the overlapping scope to ensure that integration between systems happens.
There are few skilled system integrators, and most companies use closed code programs.

Users may operate systems without proper security awareness.

Due to identified responsibilities between different involved parties within the smart city, security updates and patches may not be done.

IoT Devices and low voltage devices are targeted for attacks due to low security within their design.

Improper system usage will cause vulnerabilities within the systems.
Improper utilization of the internet.
The use of USBS and other external memory to configure these devices may cause different problems, such as malware.

The lack of qualified personnel who have expertise in implementation and operation.

Change of Management and org hierarchy will directly affect the Operation (Centralized operation, noncentralized operation. Organizational culture in case of errors or mistakes, will affect employee's behavior. Any changes in vision will cause risks since this will affect the whole project

Deficiencies in stakeholder engagement.
Many citizens resist using smart applications due to cultural or privacy concerns. Some others believe that smart applications will make them lose their jobs.

Lack of Standards, policies, still the area needs a lot of development . There is a limited awareness about the standards and policies used for smart cities.

Lack of return of investment Model, No clear strategy for return of investment of what is built, rents are high , usage of technology is not used to generate income.

There is always a lack of budget that will affect the project and may cause minimization of planned services. Also, organizations fear the huge investments in developing smart cities.

Lack of maintenance model for systems
Lack of Integration and interoperability between systems
Usage of closed code programs
Lack of security awareness
Improper security updates
IoT devices security vulnerability
Cyber attacks
Wrong Operation
Limited knowledgeable human resources and experts.
Change of Management
Organizational Process - Planning
Change of Vision
Change of hierarchy
Resistance of using the systems
Lack of communication between different stakeholders
Citizens' mindset and acceptance of digital changes
Lack of knowledge of policies, regulations, and standards
Lack of application of policies , regulations and standards
No clear business continuity plan
Lack of Data Analysis (data coming out of the sensors and analyzing them to innovate and advance the smart applications.
Lack of budget
Fear of Capital Cost
Cybersecurity risk
Technical Data and Application Risk
Network Infrastructure Risk
Data Security and Privacy
Integration Risk
Resources, Resource Management Risk
Strategic Risk
Stakeholder engagement Risk
Laws, regulations and Standards Risk
Business Continuity Risk
Financial Risk
Operations Risks
Implementation Risks
Planning Risks
Design Risks
Services continuity
Services Efficiency
Resources Productivity
Reputation
Revenue generation

Figure 4.1: Data Analysis results using the Gioia method.

4.4.1.1 Smart City Strategic Planners

As mentioned earlier, strategic planners made up 15% of the responses for this research. Candidates' profiles are mainly chief executives, managing directors, and senior smart city specialists with 25 to 30 years of experience in information technology.

The data shows that strategic planners emphasized non-technical risks, although technical risks were mentioned by some of the interviewees. Planners also mentioned organizational factors that could be the cause of risks resulting in a lack of coordination between different stakeholders, the culture of smart applications' users, and their resistance to using smart systems, which are major incidents causing stakeholder engagement risk.

One Managing Director mentioned: *"Poor communication between different stakeholders is a main source of stakeholder engagement risk that will decrease work efficiency and productivity."*

Strategic planners mentioned change management as a source of strategic risk, like the SC operators' category. Another incident causing strategic risk is the change in the organizational hierarchy or unclear hierarchy to make decisions at the right time.

Managing Director*: "Change of management is challenging when design and decisions are already taken; this may cause implementation operation disturbance and low efficiency and productivity."*

Standards, procedures, and laws for smart cities are also discussed in the interviews. The lack of awareness of standards, laws, and regulations of the country implementing the smart city is a main source of this risk.

Managing Director: *"Violating laws and regulations in the country where smart city implementation is taking place is a challenge that must be avoided since this may cause* *delays due to legal accountability and will cause smart city reputation issues."*

Regarding business continuity risk, a lack of clear planning is the main cause; the candidates mentioned that there should be a plan to encourage national companies to invest in smart city applications to avoid system discontinuity in case of force majeure circumstances.

Chief Executive mentioned*: .... "The lack of national companies may cause businesses to discontinue in case of pandemics or wars; thus, revenues will be decreased."*

A deprivation of budget is also highlighted as the main source of financial risk within this category of candidates. The effect of such incidents will minimize the scope of implementation or hinder future development.

Senior smart Campus specialist highlighted: "*Lack of budget will cause weak implementation or minimize the scope of work; accordingly, the benefits of the smart applications will decrease, revenues will be decreased, and reputation will be negatively affected due to the disturbance that may occur in services or their efficiency.*"

All participants in this category agree that the scarcity of smart city resources is the main incident causing major risks during smart city planning, implementation, and operation phases. Smart city experts with implementation, operation, and integration expertise are limited, causing a major source of resource risk.

Technical risks are discussed; smart city strategic planners believe cybersecurity, data security, and privacy are the main technical risks affecting a smart city project. The main incidents causing cybersecurity risk are improper security updates and lack of security awareness. At the same time, cyberattacks are major incidents causing data security and privacy risks.

Managing Director mentioned: *"Lack of security awareness among smart city citizens* *and employees will be a main cause of cybersecurity risk, that will cause services disturbance."*

Chief Executive declared: "*Data security and privacy risk is a high probability risk since the smart city is always connected to the internet. Cyberattacks are major incidents that will cause this risk impacting the availability of services and data and the reputation of the smart city."*

Technical data and application risk is stated, and the absence of security awareness is declared as the main incident causing this risk.

Managing Director mentioned: *"Human errors due to a lack of security awareness will cause technical data and application risk. It causes damage in smart applications and collected data from different IoT devices."*

Another discussed technical risk is integration risk. The smart city specialist stated that the deficiency in integrating different devices, the deficit in integration between smart applications, and improper integration between some hardware devices and software are major incidents causing this risk.

The chief executive mentioned: "End-*to-end process should be considered when implementing smart city applications. ...., proper integration between smart applications is a must".*

Strategic planners mentioned network infrastructure risk as negligible since most countries invest in and build proper IT networks as part of their infrastructure. Yet, they consider interoperability between systems as the main cause of this risk.

The chief executive mentioned *.... " interoperability of the used technologies must be considered at the initial design stages of the smart city. This risk will impact services that may be discontinued or disturbed."*

4.4.1.2 Smart City Implementers

This category represents 57.5% of the sample for this research. Candidates' profiles ranged from development engineers with five years of experience to smart city consultants with over 30 years of experience.

The candidates highlight technical and non-technical risks at the interviews. Identifying non-technical risks requires the discussion to start with classifying the organizational factors that can be considered as sources of risks; candidates mentioned the unclear roles and responsibilities within the smart city implementation team and different stakeholders. The coordination between different stakeholders is a main source of risk. An example from the interview scripts confirms the above results:

Senior Enterprise Application Architect: *"The key objective for the smart city is to provide services for citizens to lead a better life, ensuring sustainable usage of natural resources. To fulfill this vision, a clear responsibility matrix (RACI) should be defined between all stakeholders at the early stages of the project. ……A gap in this aspect will decrease the efficiency and productivity of working candidates in the smart city project."*

It was highlighted that if the business model of the implemented smart city was not planned and defined before implementation, and the technology model and design were decided without having a clear vision and strategy for the future business model, then there is a high probability of the risk of downgrading the scope of work to occur.

Smart City Consultant: *"When the business model for a smart city is not well defined, the return of an investment will be impacted; accordingly, this may impact the offering of new services or synchronize with accelerating technology. Also, the smart city vision is always ambitious, but implementation may end with fewer services".*

Another factor is the Change in the management of the smart city that will cause, in many cases, changes in the management vision of the smart city; this is described by:

Senior Client Service Architect: *"Change of management will cause a change in the vision and thus will affect the required deliverables and operational model. Frequent changes will negatively affect a smart city's implementation and operation in terms of efficiency and productivity."*

Although there are technical standards that can be utilized for smart city applications and hardware implementation, there is a lack of specific regulations and procedures that suit these smart applications, as mentioned below:

Senior Enterprise Application Architect highlighted: *"There are no clear procedures for facilities consumptions and rent wages, which will disturb the business model of the smart city and thus affect the investments in such projects."*

Finding the proper resources for smart city implementation and operation is a main risk factor; the number of trained personnel is scarce and may be found in different parts of the world.

This idea is supported by the ***Smart City Rollout Project Manager, who*** *mentioned that: "finding personnel with the know-how to develop, operate and integrate smart applications is rare. Accordingly, smart city services may be disturbed, leading to decreasing revenues and reputation defects."*

Another aspect investigated during the interview is the definition of incidents that cause non-technical risks. When the return-on-investment model is not well defined due to an unclear business model, then there is a risk of having a low income.

Senior Enterprise Application Architect highlighted, "*There is a lack of return of investment model; the used technology is not designed to generate income for the smart city, which means that the business model is not well defined ."*

The limited smart city resources force decision-makers to employ vendors for software development, hardware installation, and integration. Therefore, the city's technology infrastructure depends on a closed code environment. Consequently, a monopoly may occur for maintenance contracts. Also, it is difficult to change the mindset of the smart city implementation team to the operational concept.

The Smart City Rollout Project Manager *mentioned, "Vendors are controlling the hardware and the software in smart cities. Smart city systems integrators are very limited, which will lead to efficiency and productivity issues."*

A lack of budget and high cost will cause financial risk, leading to operational challenges and hindering the development and innovation of provided services within the smart city.

Regional Service Provider Director *highlighted, "Smart city is a complex project that costs millions of dollars, therefore if there is a financial risk. It may cause failure in operation and limitation in scaling the smart services, so revenue is affected."*

From the technical side, cybersecurity risk was mentioned by 65% of the interviewees of smart city implementers. Different incidents are mentioned as causes of cybersecurity risk, including lack of maintenance model for smart city systems, lack of integration between systems, improper security updates, lack of security awareness within employees and smart applications users, and low voltage devices vulnerability. This risk will disturb smart city services and affect its reputation. Examples of the scripts are mentioned as follows:

Senior Enterprise Application Architect: *"Smart city decision-makers must identify the maintenance model to avoid improper security updates for different smart applications and to minimize IoT devices' vulnerability."*

Senior Client Service Architect highlighted, *"Cybersecurity is one of the major challenges in smart cities; voltage devices are vulnerable to attacks. It will disrupt* *smart services and thus affect the reputation.”*

Technical data and application risks are other technical risks related to smart city implementation and operation. This risk is caused by multiple incidents, including power supply outages that fall into the wrong operation, lack of interoperability between systems, sharing two incidents with cybersecurity risk, lack of integration between systems, and lack of security awareness. Experience with technical data and application risk will cause service disruption. These incidents are supported by examples of candidates’ scripts as follows:

Senior Enterprise Application Architect mentioned: “*During implementation, power supply was provided to different systems using the temporary generator. These generators went down, and the applications were disconnected….”*

Chairman-CEO Smart Applications Consultancy *mentioned that: “lack of security awareness within the smart city community, including users and operators, is a primary cause of multiple risks such as …. Technical data and application risk”.*

Data security and Privacy risk are highlighted by 20% of the candidates within this group. Two major incidents were identified: the lack of security awareness and cyberattacks.

Senior Enterprise Application Architect *mentioned, "Cyber-attacks will increase if maintenance of different smart systems is not done continuously. Accordingly, data security and privacy risks may occur due to these attacks impacting provided services and data availability, thus affecting the reputation of the smart city.”*

Smart City Applications Consultant highlighted that *“human errors due to lack of security awareness and improper security training will negatively affect data security and privacy and may put the data at risk.”*

Smart city Implementers highlighted the integration risk that can result from a lack of integration between different systems (in terms of hardware and software), a lack of trained resources who can build the integration between different systems, and the usage of closed code out of the box applications, that will negatively influence smart city services.

Senior Enterprise Application Architect mentioned*: "Lack of compatibility between hardware devices and challenges in integration are main causes of integration risk, which will create weak points vulnerable to cyber-attacks."*

Smart City Roll out Project Manager: *mentioned that "Lack of system integrators and the dependency on vendors with closed code software are main incidents of integration risk."*

4.4.1.3 Smart City Operators

This category represents 15% of the sample for this research. Candidates' profiles are mainly operation managers, program managers, and lead support engineers with 15 to 30+ years of experience in information technology.

Candidates in this category highlight both technical and non-technical risks during the interviews. Discussions about organizational factors that could be causes of risks resulted in highlighting Change of management as a major incident to cause strategic risks, as highlighted by:

Program Manager: *"Change of management is a main cause of strategic risk since this will cause some resistance to the current implementation and operation model. It will influence the productivity and efficiency of the team."*

Another non-technical risk is the financial risk resulting mainly from the concern of necessary return to justify the budget to build and operate a smart city, which is considered the cost of capital.

Program Manager: *"Investors usually fear the Cost of Capital in Smart City Projects* *due to complexity. The financial risk will impact the generated revenue from smart applications and may affect the reputation of the smart city due to limited provided smart services."*

Stakeholder engagement risk is considered within this category; the candidates consider human factors to be major causes of risks, where coordination between different stakeholders is challenging and limited collaboration is a source of risk. Another incident that causes this risk is residents' reluctance to use implemented technologies. This risk is elaborated on by the lead support engineer as follows:

***Lead Support Engineer**: "The main challenge in smart city operation is lack of collaboration; people are not working together. Accordingly, the impact will be a decrease in work efficiency".*

Standards, procedures, and laws for smart cities are discussed. There are limited standards for data anthology from different smart applications. This limitation is the main source of this risk. Although some industry standards exist for data modeling, more work is needed to connect data with proper naming conventions from smart applications developed by different vendors.

***Lead Support Engineer**: "There is a dedicated team to normalize the data due to the lack of data* anthology *standards... Non-compliance with standards will lead to legalization issues that may affect the city's reputation and decrease revenues."*

Regarding business continuity risk, the absence of clear planning is a main cause; the candidates mentioned that there should be a clear vision and plan to continuously develop the smart city, considering the culture and the environment. This development can be achieved by having innovative plans for new smart applications to sustain the city.

***Lead Support Engineer highlighted:** "Culture should be considered when* *implementing and operating the smart city to ensure sustainability and acceptance of the smart city in the society; otherwise, the ability to add innovative smart services will be negatively affected; thus, the revenues will be reduced."*

Technical risks are discussed; the Smart City operation team believes that technical risks in the operational phase are minimal since the Smart City systems are constructed to be resilient, scalable, and secure to ensure smooth operation. However, candidates highlighted cybersecurity risk as the highest-rank risk. This risk is mainly caused by the vulnerability of low-voltage devices (IoT) used in most smart applications.

The ICT Operation Manager mentioned, *"Low voltage devices vulnerability is a weak point and a main cause of cybersecurity risk. It will disturb smart city services and damage the city's reputation."*

Technical data and application risk is mentioned, and lack of integration between systems is highlighted as the main incident causing this risk.

Lead Support Engineer highlighted: "*When systems are not properly integrated, connecting applications and collecting holistic data will be challenging."* In addition, integration risk is discussed based on the previous responses. The ICT Operation Manager and Lead Support Engineer mentioned that the limited number of system integrators, high turnover of system integrators during the operation stage, lack of integration between smart applications, and improper integration between some hardware devices and software are major incidents causing this risk.

Lead Support Engineer highlighted: "*When Smart city implementation is completed, many system integrators leave the project, so the risk of integration will be high. Integration risk may occur, which will cause the disturbance in smart services."*

The ICT Operation Manager mentioned, "*Different hardware and software need to be linked. Systems in different Smart buildings must be integrated into the main central* *management system to allow better control."*

4.4.1.4 Smart City Application Users

The smart city application user category also presents 12.5% of the sample for this research. Candidates in this category are IT directors using smart applications.

The discussion about non-technical risks highlighted two main risks: strategic risk and resource and resource management risk.

Change of management is the main incident causing the strategic risk, as one of the ***IT directors highlighted****: "Change of management may cause the change of vision that will affect the design and the implementation, which will be a major cause of strategic risk. That will lead to low efficiency and productivity of different teams due to changes."*

Regarding resources and resource management risk, a lack of knowledgeable resources is the main cause of this risk. ***Smart application users highlighted***: *"It is challenging to find resources with adequate skills to develop, operate, and maintain smart applications. Accordingly, efficiency, productivity, revenues, and reputation will be affected."*

Although limited technical risks are mentioned in the smart applications user's category, three main risks are highlighted: cybersecurity, technical data and applications risks, and data security and privacy risks.

From their point of view, cybersecurity is caused by improper security updates and a lack of security awareness.

The IT director mentioned, *"If the smart systems are not properly maintained from security perspectives and updates are not installed, then security vulnerability will occur, causing disturbances in the smart services."*

Head of IT mentioned: "*When users lack the awareness about security threats and* *lack the knowledge to handle smart applications, then cybersecurity risk will have a high probability to occur."*

As discussed with this group, the lack of security awareness causes technical data and application risks.

IT Director mentioned that: "*When users misuse the system, because of the absence of security knowledge, applications, and data will be at risk of cyberattacks, that may cause systems to stop, or data to be corrupted."*

Finally, data security and privacy risks are also highlighted. The candidates believe that wrong operations, cyber-attacks, and a lack of security awareness are the causes of this risk.

IT Director mentioned that "*Cyber-attacks will cause key damage to data and threaten the data privacy. It will affect the reputation of the smart city and will cause a lot of disturbance."*

Another IT Director stated, *... "Lacking the knowledge to use smart applications may wrongly operate the system, which creates vulnerability, which will cause security issues."*

IT Director mentioned that *".... Absence of security knowledge, data privacy will be at risk, ..., which will put data privacy in danger".*

Based on the 1st order themes, incidents causing each risk are summarized and grouped; as a result, the second-order themes are descended. The following Table 4.4 presents the second-order concepts, which are part of the outcomes of Phase 1 as illustrated in the suggested framework Figure 3.1

Table 4.4. The Second Order Theme Based on the Gioia Method.

No	Risk	Incidents causing risk (Components)	Component
1	Cybersecurity risk (CR)	Lack of maintenance model for systems	A
		Lack of Integration and interoperability between systems	B
		Improper security updates	C
		Lack of security awareness	D
		IoT devices vulnerability	E
		Cyber attacks	F
2	Technical Data and Application Risk (TR)	Wrong Operation	G
		Lack of Integration and interoperability between systems	B
		Lack of security awareness	D
3	Network Infrastructure risk (NR)	Lack of Integration and interoperability between systems	B
		Lack of maintenance model for systems	A
		Wrong Operation	G
		Lack of security awareness	D

No	Risk	Incidents causing risk (Components)	Component
4	Data Security and Privacy (DR)	Wrong Operation	G
		Cyber attacks	F
		Lack of security awareness	D
5	Integration Risk (IR)	Lack of Integration and interoperability between systems	B
		Limited knowledgeable human resources and experts	I
		Usage of closed code programs	J
6	Strategic Risk (SR)	Change of Management	K
		Organizational Process - Planning	L
		Change of Vision	M
		Change of hierarchy	N
7	Stakeholder engagement risk (SER)	Resistance to using the systems	O
		Lack of communication between different stakeholders	P
		Citizens’ mindset and acceptance of digital changes	Q
8	Laws, regulations, and Standards (LR)	Lack of application of policies, regulations, and standards	R

No	Risk	Incidents causing risk (Components)	Component
9	Business continuity risk (BCR)	Lack of knowledge of policies, regulations, and standards	S
		No clear business continuity plan	T
		Lack of Data Analysis	U
10	Financial Risk (FR)	Lack of budget	V
		Fear of Capital Cost	W
11	Resources, resource management risks (RMR)	Lack of knowledgeable human resources and experts	I
		Lack of budget	V

The third-order theme is extracted by grouping the risks based on the smart city project phase. Four groups are defined: design, planning, implementation, and operation risks. Design risks are mainly non-technology related: strategic risks, stakeholder engagement risks, laws, regulations, standards risks, business continuity risks, and financial risks. In the planning phase, resource and resource management risk is a major risk, in addition to strategic risk, stakeholder engagement risk, and financial risk. In the smart city implementation phase, stakeholder engagement risk, laws, regulations and standards risk, resource and resource management risk, integration risk, network infrastructure risk, and cybersecurity risk must be considered.

The smart city operation risks are mainly technology-related, including cybersecurity, technical data and application, data security and privacy, network infrastructure, and integration risks. Also, resource and resource management and stakeholder engagement risks must be studied.

The aggregated dimension is developed based on expert insights about the impacts of risks. The results show that risks will affect service continuity, efficiency, resource productivity, revenue generation, and smart city reputation.

Also, findings show that during the planning phase, smart city management should consider all technical and non-technical risks identified in this study to avoid any problems in the project's next phases. Strategic planning experts focus less on technical risks and more on non-technical risks.

Awareness of technical risks is crucial during the planning phase to avoid incidents causing major risks. Furthermore, all risks must be addressed in the implementation phase of the smart city project. Smart city implementation experts have a low concentration on non-technical risks, although they have a major effect on implementation.

During the smart city operation phase, technical risks must be addressed in combination with non-technical risks to ensure smooth and effective operation. SC operation group presented moderate awareness about the mentioned non-technical risks; accordingly, increasing awareness and including these risks in the risk management plan is fundamental for sustainable smart city operation.

The resulting impact relations from Gioia's analysis emphasize that adequate risk management will assure service continuity and support efficiency that will maintain a smart city reputation. Service continuity and revenue generation are mutually related, and their enhancement will ensure smart city sustainability. Resource productivity will enhance service efficiency and support smart city sustainability. A respectful reputation will elevate the smart city's sustainability and ensure the project's continuity. Figure 4.2 below represents the resulting impact relations, the output of Phase 1.

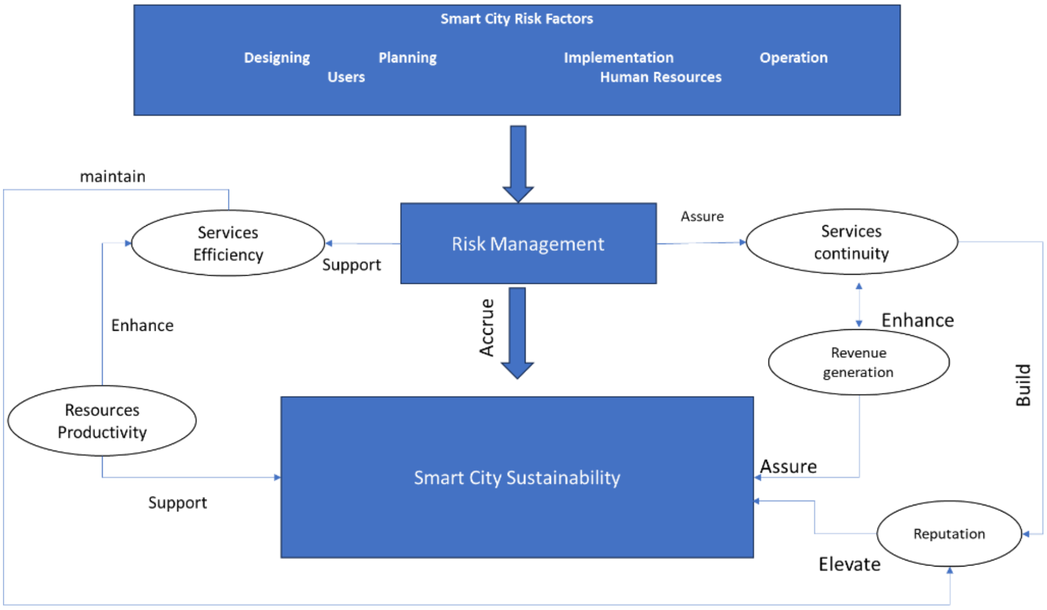


Figure 4.2: Impacts relations based on Gioia Analysis

4.4.2 Phase 2: Combined (m) calculation and risks' causal relations results

The incidents from the previous phase are used as inputs to Phase 2 to calculate the combined basic probability assignments since the basic probability assignment (m) for each incident is determined by the experts. In this Phase 2, the risks' interrelations are determined.

The interviewees are asked to rank the likelihood of incidents occurring for each risk during the interviews to be able to apply the Dempster-Shafer theory. The ranks used the Likert scale, where five is considered a very high likelihood, and one is considered a very low likelihood, as per Table 4.5.

Table 4.5. Likert scale table values.

Rank	Likert scale value
Very High	5
High	4
Medium	3
Low	2
Very Low	1

The resulting data presents the value given by each expert for incidents causing the risk that the expert mentioned during the interview. Pearson correlation coefficient is calculated between risk incidents to determine the dependence relation within incidents causing a specific risk. Table 4.6 displays a sample of the data for the Cybersecurity risk, where experts mentioned and ranked the incidents of this risk are considered. Pearson correlation coefficient is calculated, and the results verified a significant correlation between the incidents: lack of maintenance model for systems component(A), lack of integration and interoperability between systems component (B), improper security updates component (C), and lack of security awareness component (D). Meanwhile, IoT devices' vulnerability component (E) is correlated with improper security updates component (C) and lack of security awareness component (D). Other components have minor correlations. Table 4.7 presents the significant correlation results within cybersecurity risk components.

Table 4.6.Cybersecurity Risk Experts' Ranks

Cybersecurity Risk		Experts' ranks																							
Incident Name	Comp	E1	E2	E6	E7	E8	E9	E12	E14	E16	E18	E20	E21	E24	E25	E27	E30	E31	E33	E34	E35	E37	E38	E39	E40
Lack of maintenance model for systems	A	4	4	2	2	4	2	2	2	2	2	4	4	4	4	4	4	4	4	4	4	4	4	4	3
Lack of Integration and interoperability between systems	B	4	2	2	4	4	2	4	4	4	2	4	4	4	4	4	4	4	4	4	4	4	4	4	3
improper security updates	C	2	4	4	2	2	2	2	4	4	2	4	4	4	4	4	4	4	4	4	4	4	4	4	3
Lack of security awareness	D	2	4	4	2	2	4	2	2	2	2	4	4	4	4	4	4	4	4	4	4	4	4	4	3
IoT devices vulnerability	E	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3
Cyber-attacks	F	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4

Table 4.7. Significant Correlation Results Within Cybersecurity Risk Components.

Component		B	C	D
A	Pearson Correlation Value	0.451^{*}	0.473^{*}	0.592^{**}
E		-0.016	0.370	0.328

*Correlation is substantial at the 0.05 level (2-tailed).

**.Correlation is substantial at the 0.01 level (2-tailed).

The next step is to convert the scale into a percentage that will present the basic probability assignment as per the following steps used by (Murray, 2017):

1- Count the number of experts who ranked the incident as high (n).

2- Assign the weight from the Likert scale (4) for high (w).

3- Multiply the number of experts by weight (n*w).

4- Calculate the value of multiplication if all experts considered this incident as high (W).

The basic probability function is calculated as: $\frac{n*w}{W}$The basic probability assignment for Cybersecurity risk is presented in Table 4.8:

Table 4.8. Cybersecurity Risk Basic Probability Assignment Values.

Risk	Incident Name	Component	Very High	High	Moderate	Low	Very low
Cybersecurity Risk (CR)	Lack of maintenance model for systems	A	0	0.6667	0.0417	0.2917	0

Risk	Incident Name	Component	Very High	High	Moderate	Low	Very low
	Lack of Integration and interoperability between systems	B	0	0.7917	0.0417	0.1667	0
	improper security updates	C	0	0.7083	0.0417	0.2500	0
	Lack of security awareness	D	0	0.6667	0.0417	0.2917	0
	IoT devices vulnerability	E	0	0.9167	0.0417	0.0417	0
	Cyber-attacks	F	0	0.9583	0.0417	0.0000	0

The Dempster-Shafer combination rule will combine the basic belief functions of experts for several incidents to get possible combinations of incidents for each risk, and the combined basic probability assignment for each combination of incidents.

4.4.2.1 Cybersecurity Risk (CR)

Let m_1 represents the basic probability function assigned by experts considering the high occurrence of the risk (Experts H),m_2 represents the basic probability assignment assigned by experts considering the low occurrence of the risk (Experts L) and m_3 represents the basic probability assignment assigned by Experts considering Moderate risk occurrence (Experts M). As shown in Table (4.8), components from A to F are incidents causing cybersecurity risk (CR), and the basic probability assignment values for each incident

As per experts considering high values (Experts H), CR occurs due to lack of maintenance of the systems component (A) with a basic probability assignment of 0.6667, due to lack of integration and interoperability between systems component (B) with a basic probability assignment of 0.7917, due to improper security updates component (C) with a basic probability assignment of 0.7083, due lack of security awareness component (D) with basic probability assignment of 0.6667, due IoT devices vulnerability component (E) with a basic probability assignment of 0.9167, or due to Cyber-attacks component (F) with a basic probability assignment of 0.9583.

For Expert L, cybersecurity risk (CR) occurs due to component (A) with a basic probability assignment of 0.2917or due to component (B) with a basic probability assignment of 0.1667, due to component (C) with a basic probability assignment of 0.2500, due to component (D) with a basic probability assignment of 0.2917, due to component (E) with basic probability assignment of 0.0417, cyber-attack (F) incident was not rated as low accordingly plausibility using equation (3.4) is calculated for this incident. Based on this information, the steps below are used to find the combined belief function of incidents causing cybersecurity risk. Table 4.9 below is used to apply the Dempster-Shafer combination rule.

Table 4.9. Cybersecurity risk (CR) Combinations.

			Experts with High beliefs					
	Cybersecurity Risk		A	B	C	D	E	F
		m_1	0.666	0.791	0.708	0.66	0.916	0.958
	Component	m_2						
Experts with low beliefs.	A	0.291	0.194	0.230	0.206	0.194	0.267	0.279
	B	0.166	0.111	0.131	0.118	0.111	0.152	0.159
	C	0.250	0.166	0.197	0.177	0.166	0.229	0.239
	D	0.291	0.194	0.230	0.206	0.194	0.267	0.279
	E	0.041	0.027	0.032	0.029	0.027	0.038	0.039
	F	1.000	0.666	0.791	0.708	0.666	0.916	0.958

1. The combined basic probability assignment is computed for each cell by multiplying the basic probability from the related column and row.
2. The resulting values from the combination of like components appearing in two cells are added.
3. If there is a conflict between experts, one expert assigns 0 basic probability for an incident, then plausibility is to be calculated using equation (3.4).

The combined basic probability assignment m_{12} that cybersecurity risk is due to component A, and component B is 0.342; this value is derived by multiplying the basic probability assignment from the related column and row equals the 0.230 (row 1), 0.111 (row 2); the combined basic probability assignment m_{12} presents that cybersecurity risk is due to components A and B calculated by adding the two values, resulting in the combined basic probability assignment. Then, the cybersecurity risk due to components A and B is 0.230 + 0.111 = 0.341. The combinations of other incidents are shown in Table 4.10 below.

Table 4.10. Incident Combinations Causing Cybersecurity Risk (CR).

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
AA	0.19444
AB	0.34201
AC	0.37326
AD	0.38888
AE	0.29513
AF	0.94618
BB	0.13194
BC	0.31597
BD	0.34201
BE	0.18576
BF	0.82638
CC	0.17708
CD	0.37326
CE	0.25868
CF	0.94791
DD	0.19444
DE	0.29513
DF	0.94618
EE	0.03819
EF	0.95659
FF	0.95833

The highest values have resulted from the combinations of cyber-attack incident (F) and all the other incidents, lack of maintenance of the systems component (A), lack of integration and interoperability between systems component (B), improper security updates component (C), lack of security awareness component (D), and IoT devices vulnerability component (E).

Application of the Dempster-Shafer combination rule is considered for experts who believed in high values and believed in low values because the basic probability assignment resulted from experts considering moderate values to be 0.04 for all incidents, and applying the combination rule resulted in negligible values.

4.4.2.2 Technical Data and Application Risk (TR)

Technical data and applications risk is caused by multiple incidents, such as wrong operation component (G), lack of integration and interoperability between systems component (B), or lack of security awareness component (D). Correlation is calculated for the components, and a minor correlation exists between the wrong operation component (G) and the lack of integration and interoperability between systems component (B) has a value of 0.233. Other components have a slight correlation.

The combined basic probability assignment is calculated using the Dempster- Shafer combination rule; the basic probability assignment of the group of experts considering the high possibility of the incident occurring (Experts H) is presented by m_1 , while the basic probability assignment of the group of experts considering the low possibility of the incident occurring (Experts L) is presented by m_2, the basic probability function of the group of experts considering the moderate possibility of the incident occurring

(Experts M) is presented by m_3, and the basic probability function of the group of experts considering the very low possibility of the incident occurring (Experts VL) is presented by m_4 .

The Dempster combination rule is applied in two steps, where the combined basic probability assignment of (Expert H) and (Expert L) is calculated. m_{12}, then combined basic probability assignment of (Expert M) and (Expert VL) is calculated m_{34} .

The results of combining the basic probability assignment of (Expert H) and (Expert L) present considerable values for the combination of wrong operation component (G) and lack of security awareness component (D), which is equal to 0.20138. The second significant combined basic probability assignment resulted from a lack of integration and interoperability between systems component (B)and lack of security awareness component (D), equal to 0.180555. The following Table 4.11 presents combinations of incidents/combined components and combined basic probability assignments for (Experts H) and (Experts L).

Table 4.11. Incidents Combinations Causing Technical Data And Application Risk (TR) - (Expert H) And (Expert L)

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
GG	0.04166
GB	0.11111
GD	0.20138
BB	0.055555
BD	0.180555
DD	0.138888

The results of combining the basic probability assignment of (Expert M) and (Expert L) are calculated as m_{34}. For this step, the combined basic probability assignment values are significant for the combined basic probability assignment resulting from a lack of integration and interoperability between systems component (B) and lack of security awareness component (D), equal to 0.17361. The following Table 4.12 presents combinations of incidents/combined components and combined basic probability assignment for (Experts M) and (Experts VL).

Table 4.12: Incidents Combinations Causing Technical Data and Application Risk (TR) - (Expert M) And (Expert VL)

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{34})
GG	0.02777
GB	0.11111
GD	0.06250
BB	0.08333
BD	0.17361
DD	0.01388

4.4.2.3 Network Infrastructure Risk (NR)

Multiple incidents cause Network Infrastructure Risk, and it shares incidents with cybersecurity risk (CR), which are the lack of maintenance of systems (Component A), lack of integration and interoperability between systems (Component B), and lack of security awareness (Component D). While it shares the wrong operation incident (Component G) with technical data and applications risk (TR). Correlation is tested, and considerable correlation with a value of 0.944 between lack of integration and interoperability between systems (Component B) and lack of security awareness (Component D). Other incidents have a minor correlation.

The basic probability assignment of the group of experts considering the high possibility of the incident to occur (Experts H) is presented by m_1 , while the basic probability assignment of the group of experts considering the low possibility of the incident occurring (Experts L) is presented by m_2.

Dempster -Shafer combination rule is applied, where the combined basic probability assignment of (Expert H) and (Expert L) is calculated. m_{12}. Experts considering moderate probability for incidents to occur are not considered because of the resulting basic probability assignment's negligible values.

The results provide that the combined basic probability assignment is considerable for the combined basic probability assignment of lack of security awareness (Component D) with the wrong operation (Component G), with a value of 0.2975. The other significant values resulted from combining lack of maintenance of systems (Component A), lack of security awareness (Component D), lack of maintenance of systems (Component A), and wrong operation (Component G) with the value of 0.2727. Table 4.13 below presents the combined basic probability assignment causing network infrastructure risk (NR).

Table 4.13. Incidents combinations causing Network Infrastructure risk (NR) - (Expert H) and (Expert L)

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
AA	0.11570

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
AD	0.27272
AG	0.27272
BA	0.09917
BB	0.09917
BD	0.24793
BG	0.24793
DD	0.14876
GD	0.29752
GG	0.14876

4.4.2.4 Data Security and Privacy Risk (DPR)

There are three incidents causing data security and privacy risk: wrong operation (Component G), cyber-attacks (Component F), and lack of security awareness (Component D). The correlation is tested for these incidents and a minor correlation with a value of 0.202 between wrong operation (Component G), cyber-attacks (Component F), and with a value of 0.100 between cyber-attacks (Component F) and lack of security awareness (Component D).

The basic probability assignment of the group of experts considering the high possibility of the incident occurring (Experts H) is presented by m_1, while the basic probability assignment of the group of experts considering the low possibility of the incident occurring (Experts L) is presented by m_2, and the basic probability assignment of the group of experts considering the moderate possibility of the incident occurring (Experts M) is presented by m_3. Dempster -Shafer combination rule is applied, where the combined belief assignment of (Expert H) and (Expert L) is calculated as m_{12}.

In this risk, none of the experts considered a low probability of having a cyber-attack incident (Component F). Accordingly, plausibility is calculated for this value using equation (3.4) (Sentz & Ferson, 2002). For a cyber-attack (Component F), when combined with a wrong operation (Component G), the combined basic probability assignment has a high value of 0.783933. When combined with a lack of security awareness (Component D), the combined basic probability assignment is elevated with a value of 0.88088. The results are presented below in Table 4.14.

Table 4.14. Combined basic probability assignment for Data Security and Privacy Risk (DPR) - (Expert H) and (Expert L)

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
GG	0.07202
GF	0.78393
GD	0.24653
FF	0.94736
FD	0.88088
DD	0.16620

4.4.2.5 Integration Risk (IR)

There are multiple incidents causing integration risk, lack of integration and interoperability between systems (Component B), limited knowledgeable human resources and experts (Component I), and the usage of closed code programs (Component J). The correlation coefficient between these components is calculated.

The results present a significant relationship between lack of integration and interoperability between systems (Component B) and limited knowledge of human resources and experts (Component I), with a coefficient of 0.714.

Also, the lack of integration and interoperability between systems (Component B) has a substantial connection with using closed code programs (Component J). The value of the coefficient is 0.535.

Dempster - Shafer combination rule is applied to calculate the combined basic probability assignment. The basic probability assignments for (Expert H) that are presented by m_1, and basic probability assignments (Experts L), which are presented by m_2. The results declare substantial combined basic probability assignment when combining the lack of integration and interoperability between systems (Component B) and limited knowledgeable human resources and experts (Component I). The value for this combination is 0.26222. The value of the combined basic probability assignment rises to 0.368888 when combining the lack of integration and interoperability between systems (Component B) and the usage of closed code programs (Component J). The results are presented in Table 4.15:

Table 4.15. Combined basic probability assignment for Integration Risk (IR) - (Expert H) and (Expert L)

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
BB	0.11555
BI	0.26222
BJ	0.36888
II	0.13333
IJ	0.34222

JJ	0.20000

Some experts provided moderate basic probability assignments for incidents to occur. However, these values are not considered because of the resulting basic probability assignment's negligible numerical value.

4.4.2.6 Strategic Risk (SR)

Experts introduce four incidents causing strategic risk, which are change of management (Component K), organizational process and planning (Component L), changes in vision (Component M), and change of hierarchy (Component N). The correlation coefficient is calculated, and the change of management (Component K) is correlated with organizational process and planning (Component L) with a value of 0.464, with changes in vision (Component M) with a value of 0.601, and with the change of hierarchy (Component N) with the value 0.632.

Dempster- Shafer combination rule is applied in two stages. The first stage of the basic probability assignment of the group of experts considering the very high possibility of the incident to occur (Experts VH) that is presented by m_1, and basic probability assignment of the group of experts considering the moderate possibility of the incident occurring (Experts M), which is presented by m_2.

This stage resulted in negligible combined basic probability assignments, as presented in Table 4.16. These values will not be used in the calculations.

Table 4.16.Combined Basic Probability Assignment For Strategic Risk (SR) - (Expert VH) And (Expert M)

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
KK	0.01134
KL	0.02646
KM	0.01890
KN	0.02268
LL	0.01512
LM	0.02268
LN	0.02646
MM	0.00756
MN	0.01890
NN	0.01134

Then, the combination rule is applied to the basic probability assignment of the group of experts considering the high possibility of the incident occurring (Experts H) that is presented by m_3 , and basic probability assignment of the group of experts considering the low possibility of the incident occurring (Experts L), which is presented by m_4. This stage resulted in combined basic probability assignments m_{34}, as presented in table 4.17.

The significant value results from combining a change of management (Component K) with a change of hierarchy (Component N). The combined basic probability assignment has a value of 0.23818.

Other high values of combined basic probability assignment resulted from combining organizational process and planning (Component L) and change of hierarchy (Component N) with the value of 0.19962 and from combining change of hierarchy (Component N) and changes in vision (Component M) with the value 0.19281.

Table 4.17: Combined basic probability assignment for Strategic Risk (SR) - (Expert H) and (Expert L)

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{34})
KK	0.09829
KL	0.17088
KM	0.14744
KN	0.23818
LL	0.07258
LM	0.13459
LN	0.19962
MM	0.04914
MN	0.19281
NN	0.13610

4.4.2.7 Stakeholder Engagement Risk (SER)

Experts state three incidents causing stakeholder engagement risk: resistance to using the systems (Component O), lack of communication between different stakeholders (Component P), and citizens' mindset and acceptance of digital changes (Component Q). Correlation results present a substantial relationship with a value of 0.657 between the resistance to using the systems (Component O) and the lack of communication between stakeholders (Component P). Also, the relationship between resistance to using the systems (Component O) and citizens' mindset and acceptance of digital changes (Component Q) is considerable, with a value of 0.885.

Dempster- Shafer combination rule is applied in two stages. The first stage of the basic probability assignment of the group of experts considering the very high possibility of the incident to occur (Experts VH) that is presented by m_1, and basic probability assignment of the group of experts considering the moderate possibility of the incident occurring (Experts M), which is presented by m_2. This stage resulted in negligible combined basic probability assignments, as presented in Table 4.18. These values will not be used in the calculations.

Table 4.18 Combined Basic Probability Function for Stakeholder Engagement Risk (SER)- (Expert VH) And (Expert M).

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
OO	0.0192
OP	0.0384
OQ	0.032
PP	0.0192
PQ	0.032
QQ	0.0128

The second stage is applying the combination rule on the basic probability assignment of the group of experts considering the high possibility of the incident occurring (Experts H) that is presented by m_3, and basic probability assignment of the group of experts considering the low possibility of the incident occurring (Experts L), which is presented by m_4. This stage resulted in combined basic probability assignments m_{34}, as presented in table 4.19.

Significant combinations resulted from joining resistance when using the systems (Component O). Lack of communication between different stakeholders (Component P) with a value of 0.2416, combining resistance to using the systems (Component O) and citizens' mindset and acceptance of digital changes (Component Q) with a value of 0.2592, and joining lack of communication between different stakeholders (Component P), and citizens' mindset and acceptance of digital changes (Component Q) with the value 0.248.

Table 4.19 Combined Basic Probability Function For Stakeholder Engagement Risk (SER)- (Expert H) and (Expert L).

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{34})
OO	0.1152
OP	0.2416
OQ	0.2592
PP	0.048
PQ	0.248
QQ	0.144

4.4.2.8 Laws, Regulations, and Standards Risk (LR)

Experts declare two incidents causing risk for laws, regulations, and standards: lack of application of policies, regulations, and standards (Component R) and lack of knowledge of policies, regulations, and standards (Component S). Correlation is tested between the two components, and the results present a substantial relationship between the two components with a value of 0.657.

Application of the Dempster -Shafer combination rule is performed on the basic probability assignment of the group of experts considering the high possibility of the incident to occur (Experts H) that is presented by m_1 , and basic probability assignment of the group of experts considering the low possibility of the incident occurring (Experts L), which is presented by m_2. The resulting combined basic probability assignment demonstrates significant value when combining the lack of application of policies, regulations, and standards (Component R) and the lack of knowledge of policies, regulations, and standards (Component S) with a value of 0.20661. Single incidents have a basic probability assignment of 0.10330. Table 4.20 presents the results.

Table 4.20 Combined basic probability function for Laws, Regulations, and Standards Risk (LR)- (Expert H) and (Expert L)

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
RR	0.10330
RS	0.20661
SS	0.10330

The basic probability assignment m_3 of experts considering moderate probability (Expert M) resulted in very low values, which will not be used in phase 3 calculations.

4.4.2.9 Business Continuity Risk (BCR)

According to experts ' beliefs, two incidents are causing Business Continuity risk: lack of a clear business continuity plan (Component T) and lack of data analysis in analyzing collected data from different sensors to create innovative and advanced smart applications (Component U). The two components are independent since the correlation coefficient is 0.

Application of the Dempster – Shafer combination rule is performed in two stages. The first stage of the basic probability assignment of the group of experts considering the very high possibility of the incident to occur (Experts VH) that is presented by m_1, and basic probability assignment of the group of experts considering the moderate possibility of the incident occurring (Experts M), which is presented by m_2 to get the combined basic probability assignment m_{12}. The resulting values are considered low and presented in Table 4.21.

Table 4.21 Combined Basic Probability Assignment Business Continuity Risk (BCR)-(Expert VH) And (Expert M).

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
TT	0.04
TU	0.06
UU	0.02

The application of the combination rule on the basic probability assignment of the group of experts believing a high possibility of the incident to occur (Experts H) that is presented by m_3, and basic probability assignment of the group of experts considering the low possibility of the incident occurring (Experts L), which is presented by m_4 to get the combined basic probability assignment m_{34} , provides higher values, as presented in Table 4.22.

Where combining the lack of a clear business continuity plan (Component T) and lack of data analysis in terms of analyzing collected data from different sensors to create innovative and advanced smart applications (Component U) results in a value of combined basic probability assignment of 0.1, that is higher than the resulted combination when combining the same incidents when considering basic probability assignments of (Expert VH) and (Expert M).

Table 4.22 Combined Basic Probability Assignment Business Continuity Risk (BCR)-(Expert H) And (Expert L).

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{34})
TT	0.05
TU	0.1
UU	0.05

4.4.2.10 Financial Risk (FR)

The experts mentioned two incidents causing financial risk: a lack of budget (Component V) and fear of capital costs (Component W). Correlation is tested, and the results present a significant relation between the two incidents with a value of 0.851. Dempster – Shafer combination rule is performed, the basic probability assignment of the group of experts considering the high possibility of the incident to occur (Experts H) that is presented by m_1 , and basic probability assignment of the group of experts considering the low possibility of the incident (Experts L) that is presented by m_2. The combined basic probability assignment m_{12} is significant when combining the two components, lack of budget (Component V) and fear of capital cost (Component W), with a value of 0.204. In contrast, the value rises for combined basic probability assignment of fear of capital cost (Component W) is calculated. It has a value of 0.24. The results are presented in Table 4.23. When the combination rule is applied to calculate the combination of basic probability assignment of the group of experts considering the moderate possibility of the incident (Experts M) $m_3$with the combined basic probability assignment m_{12}, the resulting values are very low, so they will not be considered in the calculations.

Table 4.23. Combined Basic Probability Assignment Financial Risk (FR)-(Expert H) And (Expert L).

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
VV	0.102041
VW	0.204082
WW	0.24

4.4.2.1 Resources and Resource Management Risk (RMR)

Experts stated that there are two incidents causing resources and resource management risk: lack of knowledgeable resources and experts (Component I) and lack of budget (Component V). Correlation is tested, and the results present a minor relationship between the two components with a value of 0.273.

Application of the Dempster – Shafer combination rule is performed on the basic probability assignment of the group of experts considering the high possibility of the incident to occur (Experts H) that is presented by m_1 , and basic probability assignment of the group of experts considering the low possibility of the incident occurring (Experts L), which is presented by m_2.

The results present a combined basic probability assignment with a value of 0.09949 when combining a lack of knowledgeable resources and experts (Component I) and a lack of budget (Component V). Other combinations are presented in Table 4.24. When the combination is applied to calculate the combination of basic probability assignment of the group of experts considering the moderate possibility of the incident (Experts M) $m_3$with the combined basic probability assignment m_{12}, the resulting values are very low, so they will not be considered in the calculations.

Table 4.24. Combined Basic Probability Assignment Resource and Resource Management Risk (RMR) (Expert H) and (Expert L).

Incidents Combinations /Combined Components	Combined basic probability assignment (m_{12})
II	0.098214
IV	0.09949
VV	0.020408

The resulting combinations from this phase are inputs to calculate the joint probability of risk scenarios. The identified risk scenarios are based on experts' interviews and the common incidents between risks. The following section provides the defined risk scenarios for a smart city project.

4.4.3 Phase 3: Risk Scenarios Identification and Evaluation Results

To assess smart city risks resulting from the initial analysis of the Gioia method. Bayesian Network is used as a probabilistic modeling method to graph relationships between identified risks during expert interviews (Shishkina, 2015).

The graphical model combines the experts' combined beliefs resulting from applying the Dempster-Shafer theory as a result of Phase 2 section 4.4.2. In this section, risk scenarios are graphed based on the experts' interviews and discussions about different risks and relations between them. Then, the scenarios are evaluated using an Analytical Hierarchical Process (AHP). The mechanism to reach the results is discussed in section 3.2.3.

4.4.3.1 Smart City Design Phase Risks' Scenarios

The design phase risk resulted from stakeholder engagement risks(SER), strategic risk (SR), financial risk (FR), business continuity risk (BCR) and lows, and regulations and standards risk (LR). This result is presented in the Gioia method results from Figure 4.1. The graphical presentation of the relationship for this scenario, scenario one, is presented in Figure 4.3

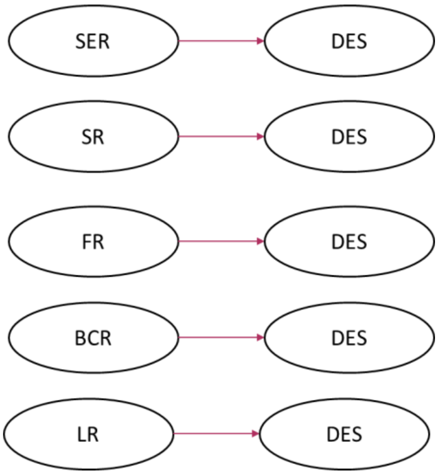


Figure 4.3 Design Phase Risk Scenario 1

The joint probability of this scenario is calculated, considering the combination of incidents causing each risk, where combinations with a value less than 10% are not considered since the values will be negligible.

The formula of Bayesian theory and joint probability (3.14) is used, and the marginal probability of design risk occurring is calculated by counting the number of experts who mentioned any of the risks causing design phase risk.

The following paragraph will explain the calculation for one case in this scenario :

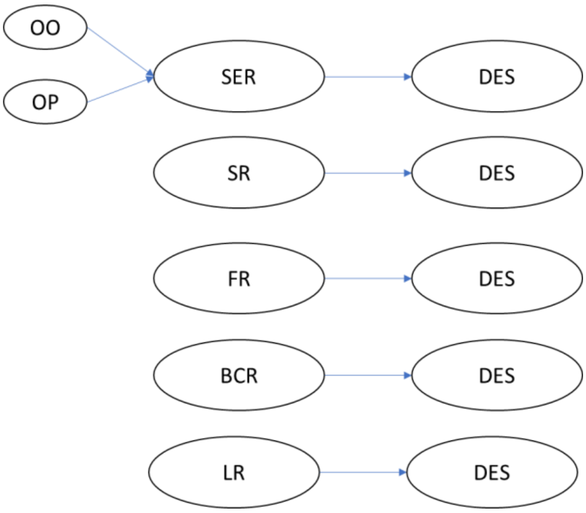


Figure 4.4 Detailed Design Risk Scenario1

1. Let U be the event that stakeholder engagement risk (SER) occurs due to combined incidents OO and combined incidents OP, i.e., U = OO ∩ OP. Using Bayes' theorem, we have:

$$P(SER|U) = \frac{P(U|SER)P(SER)}{P(U)}$$

P(U|SER) is the probability of SER risk due to the combined incidents OO and OP, and P(SER) is the marginal probability of risk SER, which is 0.625.

To calculate P(U|SER), we can use OO and OC as independent events given SER.

P(U|SER) =P(OO|SER) P(OP|SER)

P(OO|SER) and P(OP|SER) are calculated using the Dempster-Shafer theory as per table 4.17.

P(U|SER) = 0.027832

To calculate P(U), we can use the law of total probability and the fact that SER and ¬SER are separate events, according to the below formula:

P(U)=P(U|SER) P(SER)+P(U|¬SER) P(¬SER)

P(U|¬SER) is the probability of combined incidents B and C happening, given that SER does not occur, and $P(\neg SER)$ is the probability of SER not occurring.

2. Given that OO and OP are independent events given ¬SER, the formula below calculates $P(U|\neg SER)$.

$$P(U|\neg SER) = P(OO|\neg SER)\ P(OP|\neg SER)$$

$$P(U|\neg SER) = 0.972167$$

P(U) is calculated using the equation (3.12), then the P(SER|U) is calculated using the equation (3.10).

$$P(U) = P(U|SER)\ P(SER) + P(U|\neg SER)\ P(\neg SER)$$

$$= 0.027832 * 0.625 + 0.972167 * 0.375$$

$$= 0.38195808$$

Then, the probability of SER to occur due to OO and OP is calculated to equal 0.04554217.

The probability of design risk DES to occur due to stakeholder engagement risk(SER) due to OO and OP incidents is calculated using equation (3.10).

P(DES| SER) = 0.042186717. Table 4.25 will provide the different cases for this scenario.

Table 4.25 Causal Probability for Design Risk.

Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(SER|U)	P(DES| SER)
SER	SER Due to OO, OP	0.04554	0.04219
	SER Due to OQ, PP	0.02057	0.01901
	SER Due to PQ, QQ	0.05814	0.05390
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(SR|U)	P(DES| SR)
SR	SR Due to KL, KM	0.04130	0.03825
	SR Due to KN, LM	0.05231	0.04848
	SR Due to LN, MN	0.06255	0.05801
	SR Due to NN	0.20797	0.19510
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(FR|U)	P(DES| FR)
FR	FR Due to VV, VW	0.01132	0.01046
	FR Due to WW	0.14533	0.13567
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(BCR|U)	P(DES| BCR)
BCR	BCR Due to TU	0.03571	0.03306
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(BCR|U)	P(DES| BCR)
LR	LR Due to RR, RS	0.02596	0.02401
	LR Due to SS	0.12343	0.11503

To calculate the joint probability of the design phase risk to occur due to SER, SR, FR BCR, and LR, the maximum probability of design phase risk to occur due to each risk is used, considering the worst-case scenario. Accordingly, the probability of design phase risk to happen due to SER, SR, FR, BCR, and LR is calculated using equation (3.14) as negligible $\approx 5.4 \times 10^{-6}$.

The probability of the first scenario is calculated considering that each risk may occur due to one combination of incidents. Equation (3.14) is used, and the maximum probability value from Table 4.26 is considered to calculate the worst-case scenario.

Accordingly, the probability of design phase risk due to SER, SR, FR, BCR, and LR equals 0.000115747.

Table 4.26: Causal Probability for Design Phase Risk Considering One Combination of Incidents.

Risk	Risk Due to Combined Incidents	P(SR| Combined Incidents)	P(DES|SR)
SR	SR Due to KL	0.255685032	0.240752084
	SR Due to KN	0.342577488	0.324784122
	SR Due to LN	0.29362696	0.277303642
	SR Due to NN	0.20797227	0.195095516
	SR Due to KM	0.223752151	0.210157618
	SR Due to LM	0.20585174	0.193074274
	SR Due to MN	0.284757119	0.268739297
Risk		P(SER| Combined Incidents)	P(DES|SER)
SER	SER Due to OO	0.178306092	0.166879129
	SER Due to OP	0.346807533	0.328904378
	SER Due to OQ	0.36834925	0.349929798
	SER Due to PP	0.07751938	0.071985603
	SER Due to QQ	0.218978102	0.205596802
	SER Due to PQ	0.354691076	0.336590662
Risk		P(LR| Combined Incidents)	P(DES|LR)
LR	LR Due to RR	0.123429084	0.115026665
	LR Due to RS	0.24143986	0.227085054

Risk	Risk Due to Combined Incidents	P(SR| Combined Incidents)	P(DES|SR)
	LR Due to SS	0.123429084	0.115026665
Risk		P(BCR| Combined Incidents)	P(DES|BCR)
BCR	BC Due to TU	0.035714286	0.033057851
Risk		P(FR| Combined Incidents)	P(DES|FR)
FR	FR Due to VV	0.057660626	0.053462322
	FR Due to VW	0.121317158	0.113039968
	FR Due to WW	0.14532872	0.135666218

The results are more reasonable when considering one combination because the combined basic probability assignment results from the Dempster- Shafer combination rule, which is considered a strict AND operation. Accordingly, applying Bayesian theory will apply one more AND, resulting in a lower probability when considering more than one combined incident.

The second scenario consideration for design phase risk to occur is due to financial risk (FR) that may result from the cascaded effect of lows, regulations, standards risk (LR), and business continuity risk (BCR). Figure 4.5 presents this scenario.

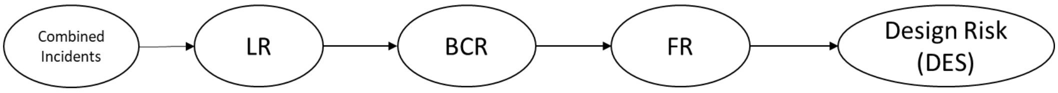


Figure 4.5 Design phase Risk Scenario 2

To calculate the probability of design risk to occur, the probability of lows, regulations, and standards risk (LR) because of the combined incidents (RS), which is the lack of knowledge of policies, regulations, and standards, and lack of application of policies, regulations, and standards using Bayes theory equation (3.10). P(LR| RS) = 0.24144. The combined incidents RS is used since it has the maximum probability of occurring.

The probability of Design risk due to the second scenario is calculated using the equation (3.14) as follows in Table 4.27:

P (LR, BCR, FR, DES) = P(DES|FR). P(FR|BCR). P(BCR|LR) .P(LR) = 0.001595

The values are summarized as follows :

Table 4.27.The Values Used to Calculate Design Phase Risk Scenario 2

Probability	Value	Source
P(DES|FR)	0.13566	Maximum value of this risk (Table 4.26)
P(FR|BCR)	0.21428	Calculated statistically from the data.
P(BCR|LR)	0.22727	Calculated statistically from the data.
P(LR)	0.24144	This is calculated as P(LR| RS) using equation (3.10)

The probability of design phase risk due to the second scenario is insignificant.

The third scenario for the design phase risk to occur is stakeholder engagement risk (SER), which may result from the effect of strategic risk (SR). The Strategic risk probability is calculated using Bayesians' theory 3.10. Since it occurs due to multiple combined incidents, the highest value is used to calculate the probability of this scenario arising.

The graphical presentation is provided in Figure 4.6.

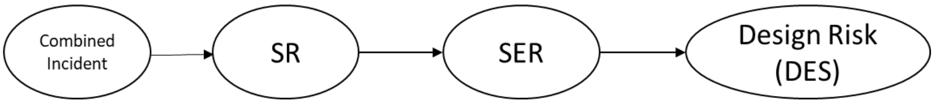


Figure 4.6 Design Phase Risk Scenario 3

To calculate the probability of Design risk to occur in this scenario, the probability of strategic risk (SR) because of the combined incidents (KN), which are the change of management (component K) and change of hierarchy (component N), is calculated using equation (3.10) P(SR| KN) = 0.342577. KN is used for combined incidents since it has the maximum occurrence probability.

The probability of Design phase risk due to the third scenario is calculated using the equation (3.14) as follows :

P (SR, SER, DES) = P(DES|SER). P(SER|SR).P(SR) = 0.0863

The values are summarized in Table 4.28 as follows :

Table 4.28. The Values Used to Calculate Design Phase Risk Scenario 3

Probability	Value	Source
P(DES|SER)	0.34992	Maximum value of this risk (Table 4.26)
P(SER|SR)	0.72	Calculated statistically from the data.
P(SR)	0.342577488	This is calculated as P(SR| KN) using equation (3.10)

The probability of design phase risk due to the third scenario is significant compared to the first and the second scenarios.

The probability of Design phase risk to occur is summarized in Table 4.29 as follows:

Table 4.29. Design Phase Risk Probabilities

Scenario	P(DES| Scenario)
Scenario 1	0.000115747
Scenario 2	0.001595161
Scenario 3	0.086312211

4.4.3.2 Smart City Planning Phase Risks' Scenarios

The planning phase risk resulted from stakeholder engagement risks(SER), strategic risk (SR), financial risks (FR), and resource and resource management risks (RMR). The graphical presentation of the causal relationship for this scenario, scenario one, is presented in Figure 4.7

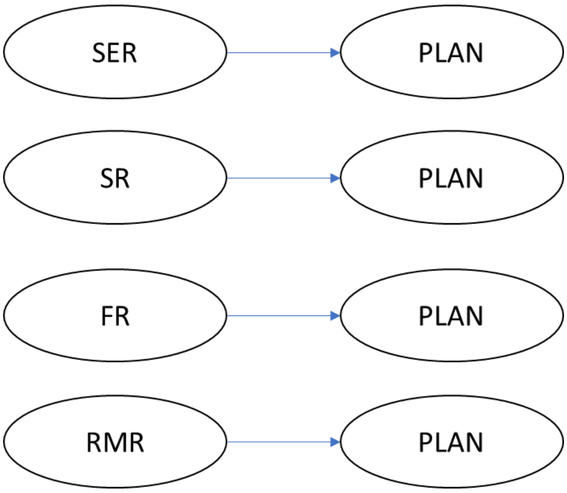


Figure 4.7 Planning Phase Risk Scenario1

The joint probability of this scenario is calculated, considering the combination of incidents causing each risk, where combinations with a value less than 10% are not considered since the values will be negligible.

The formulas of Bayesian theory and joint probability (3.14) are used. The marginal probability of planning phase risk occurring is calculated by counting the number of experts who mentioned any of the risks causing planning phase risk.

The following Table 4.30 represents the probabilities of planning phase risk occurrence due to scenario 1.

Table 4.30:Planning Phase Risk Scenario 1 Probabilities.

Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(SER|U	P(PLAN| SER)
SER	SER Due to OO, OP	0.04554	0.06064
	SER Due to OQ, PP	0.02057	0.02762
	SER Due to PQ, QQ	0.05814	0.07707
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(SR|U)	P(PLAN| SR)
SR	SR Due to KL, KM	0.04130	0.055075
	SR Due to KN, LM	0.05231	0.069492
	SR Due to LN, MN	0.06255	0.082793
	SR Due to NN	0.20797	0.262133
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(FR|U)	P(PLAN| FR)
FR	FR Due to VV, VW	0.01132	0.01525
	FR Due to WW	0.14533	0.187028
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(RMR|U	P(PLAN | RMR)
RMR	RMR Due to IV	0.03571	0.258587

To calculate the joint probability of the planning phase risk to occur due to SER, SR, FR, and RMR, the maximum probability of planning phase risk to occur due to each risk is used, considering the worst-case scenario. Accordingly, the probability of planning phase risk due to SER, SR, FR, and RMR is calculated using equation (3.14) as very low ≈ 0.00056183. The joint probability is calculated, considering that one combined incident causes each risk, and the combination of the highest value is used considering worst-case occurrence; thus, the value is 0.007677522. Table 4.31 presents the probabilities for each case.

Table 4.31. Planning Phase Risk Scenario 1 Probabilities Considering One Combined Incident.

Risk	Risk Due to Combined Incidents	P(SR| Combined Incidents)	P(PLAN|SR)
SR	SR Due to KL	0.25568	0.31729
	SR Due to KM	0.22375	0.28056
	SR Due to KN	0.34257	0.41349
	SR Due to LM	0.20585	0.25964
	SR Due to LN	0.29362	0.35995
	SR Due to MN	0.28475	0.35007
	SR Due to NN	0.20797	0.26213
Risk		P(SER| Combined Incidents)	P(PLAN|SER)
SER	SER Due to OO	0.17830	0.22695
	SER Due to OP	0.34680	0.41804
	SER Due to OQ	0.36834	0.44101
	SER Due to PP	0.07751	0.10208
	SER Due to PQ	0.35469	0.42648
	SER Due to QQ	0.21897	0.27500
Risk		P(FR| Combined Incidents)	P(PLAN|FR)
FR	FR Due to VV	0.05766	0.07645

Risk	Risk Due to Combined Incidents	P(SR| Combined Incidents)	P(PLAN|SR)
	FR Due to VW	0.12131	0.15739
	FR Due to WW	0.14532	0.18702
Risk		P(RMR| Combined Incidents)	P(PLAN|RMR)
RMR	RMR Due to IV	0.20495	0.25858

The second scenario consideration for planning phase risk is the occurrence of planning risk due to financial risk (FR) that may result in the cascaded effect of resources resource management risk (RMR). Figure 4.8 presents this scenario.

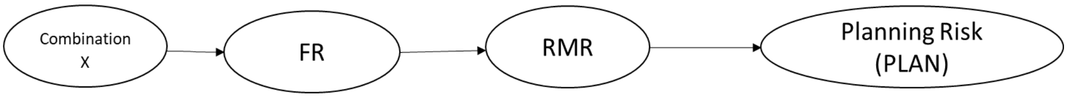


Figure 4.8: Planning Phase Risk Scenario 2

The probability of this scenario is calculated using equation 3.14 and denoted as :

P (FR, RMR, PLAN) = P(PLAN|RMR). P(RMR|FR).P(FR) = 0.013421. The value is calculated using the probabilities as shown in Table 4.32.

Table 4.32: The Values Used to Calculate Planning Phase Risk Scenario 2

Probability	Value	Source
P(PLAN|RMR)	0.25858	Maximum value of this risk (Table 4.31)
P(RMR|FR)	0.35714	Calculated statistically from the data.
P(FR)	0.14532	This is calculated as P(FR| WW) using equation (3.10)

The third scenario for planning phase risk occurs due to stakeholder engagement risk (SER), which may result from the effect of strategic risk (SR). The Strategic risk probability is calculated using Bayesian theory (3.10.) Since it occurs due to multiple combined incidents, the highest value is used to calculate the probability of this scenario arising.

The graphical presentation is provided in Figure 4.9.

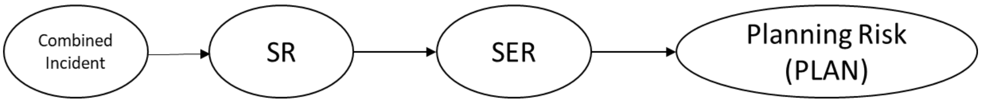


Figure 4.9 Planning Phase Risk Scenario 3

To calculate the probability of planning phase risk to occur due to this scenario, the probability of strategic risk (SR) because of the combined incidents (KN), which are the change of management (component K) and change of hierarchy (component N), is calculated using equation 3.10. P(SR| KN) = 0.34258. KN is used for combined incidents since it has the maximum occurrence probability.

The probability of planning phase risk due to the third scenario is calculated using the equation (3.14) as follows :

P (SR, SER, PLAN) = P(PLAN|SER). P(SER|SR).P(SR)   = 0.10877

The values are summarized as follows in table 4.33 :

Table 4.33. The Values Used to Calculate Planning Phase Risk Scenario 3

Probability	Value	Source
P(PLAN|SER)	0.44101	Maximum value of this risk (Table 4.29)
P(SER|SR)	0.72	Calculated statistically from the data.

P(SR)	0.34257	This is calculated as P(SR| KN) using equation 3.10

The third scenario results in the highest probability of planning phase risk. The following Table 4.34 will present a summary of implementation phase risk probabilities due to different scenarios:

Table 4.34:Planning Phase Risk Probabilities.

Scenario	P(PLAN| Scenario)
Scenario 1	0.007677
Scenario 2	0.013421
Scenario 3	0.10877

4.4.3.3 Smart City Implementation Phase Risks' Scenarios

The implementation phase risk resulted from seven risks, namely cybersecurity risk (CR), network infrastructure risk (NR), integration risk (IR), stakeholder engagement risks(SER), resource and resource management risks (RMR), laws, regulations, and standards risk (LR), and financial risks (FR). The graphical presentation of the causal relationship for this scenario, scenario one, is presented in Figure 4.10

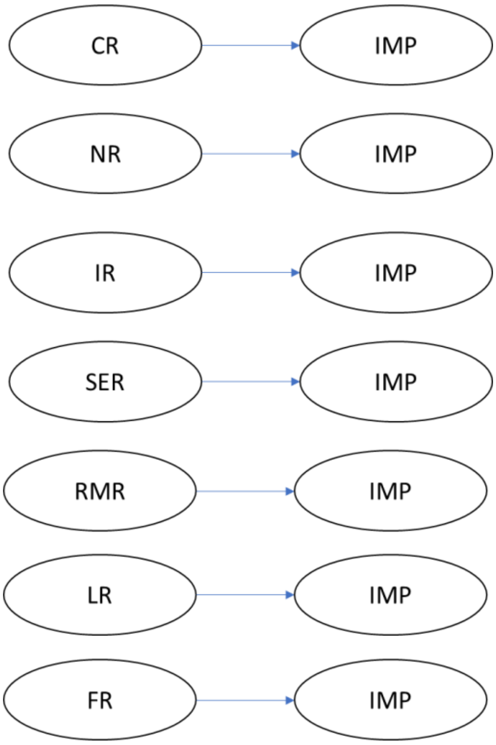


Figure 4.10 Implementation Phase Risk Scenario1

The joint probability of this scenario is calculated, considering the combination of incidents causing each risk, where combinations with a value less than 10% are not considered since the values will be negligible.

The formula of Bayesian theory and joint probability (3.14) is used, and the marginal probability of implementation phase risk occurring is calculated by counting the number of experts who mentioned any of the risks causing implementation phase risk.

Table 4.35 represents the probabilities of implementation phase risk occurrence due to scenario 1.

Table 4.35.Implementation Phase Risk Scenario 1 Probabilities.

Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(CR| U)	P(IMP|CR)
CR	CR Due to AE, AF	0.36756	0.36425
	CR Due to BF, CC	0.20454	0.20223
	CR Due to CF, DD	0.25315	0.25045
	CR Due to DE, DF	0.36756	0.36425
	CR Due to AB, AD	0.18707	0.18490
	CR Due to EF, FF	0.94291	0.94213
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(NR| U)	P(IMP|NR)
NR	NR Due to BG, BD	0.02424	0.02391
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(IR| U)	P(IMP|IR)
IR	IR Due to IJ	0.23790	0.23532
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(RMR| U)	P(IMP|RMR)
RMR	RMR Due to IV	0.20495	0.20264
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(SER| U)	P(IMP|SER)
SER	SER Due to OO, OP	0.04554	0.04493
	SER Due to OQ, PP	0.02057	0.02028
	SER Due to PQ, QQ	0.05814	0.05736
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(LR| U)	P(IMP|LR)
LR	LR Due to RR, RS	0.02596	0.02561
	LR Due to SS	0.12343	0.12189
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(FR| U)	P(IMP|FR)
FR	FR Due to VV, VW	0.01132	0.01116
	FR Due to WW	0.14533	0.14356

To calculate the joint probability of the implementation phase risk to occur due to CR, NR, IR, RMR, SER, LR, and FR, the maximum probability of implementation phase risk to occur due to each risk is used, considering the worst-case scenario. Accordingly, the probability of planning phase risk due to CR, NR, IR, RMR, SER, LR, and FR is calculated using equation (3.14)as very low ≈ 0.00000108. The joint probability is calculated, considering that one combined incident causes each risk, and the combination of the highest value is used considering worst-case occurrence; thus, the value is calculated as 0.000063627. Table 4.36 presents the probabilities for each case.

Table 4.36: Implementation Phase Risk Scenario 1 Probabilities Considering One Combined Incident.

Risk	Risk Due to Combined Incidents	P(CR| Combined Incidents)	P (IMP|CR)
CR	CR Due to AC	0.47184	0.46828
	CR Due to AD	0.48837	0.48480
	CR Due to AE	0.38578	0.38240
	CR Due to AF	0.96346	0.96296
	CR Due to BF	0.87715	0.87560
	CR Due to CC	0.24402	0.24139
	CR Due to CF	0.96466	0.96417
	CR Due to DD	0.26582	0.26304
	CR Due to DE	0.38578	0.38240
	CR Due to DF	0.96346	0.96296
	CR Due to EF	0.97064	0.97023
	CR Due to FF	0.97183	0.97144
Risk	Risk Due to Combined Incidents	P(NR| Combined Incidents)	P (IMP|NR)

NR	NR Due to BG	0.11115	0.10974
	NR Due to BD	0.11115	0.10974
Risk	Risk Due to Combined Incidents	P (IR |Combined Incidents)	P (IMP|IR)
IR	IR Due to IJ	0.23790	0.23532
Risk	Risk Due to Combined Incidents	P (RMR |Combined Incidents)	P (IMP|RMR)
RMR	RMR Due to IV	0.20495	0.20264

Risk	Risk Due to Combined Incidents	P (SER| Combined Incidents)	P (IMP|SER)
SER	SER Due to OO	0.17831	0.17622
	SER Due to OP	0.34681	0.34358
	SER Due to OQ	0.36835	0.36503
	SER Due to PP	0.07752	0.07650
	SER Due to PQ	0.35469	0.35143
	SER Due to QQ	0.21898	0.21654
Risk	Risk Due to Combined Incidents	P (LR| Combined Incidents)	P (IMP|LR)
LR	LR Due to RR	0.12343	0.12189
	LR Due to RS	0.24144	0.23883
	LR Due to SS	0.12343	0.12189
Risk	Risk Due to Combined Incidents	P (FR| Combined Incidents)	P (IMP|FR)
FR	FR Due to VV	0.05766	0.05689
	FR Due to VW	0.12132	0.11980
	FR Due to WW	0.14533	0.14356

The second scenario consideration for implementation phase risk is caused by cybersecurity risk (CR), resulting in the cascaded effect of integration risk (IR). Figure 4.11 presents this scenario.

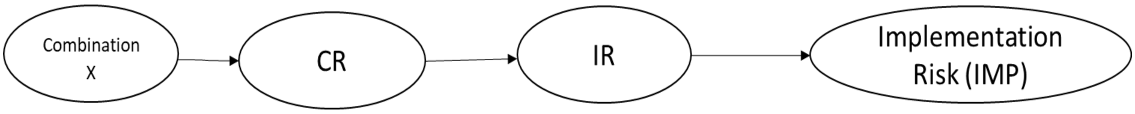


Figure 4.11: Implementation Phase Risk Scenario 2

The probability of this scenario is calculated using equation (3.14)and denoted as :

P (CR, IR, IMP) = P(IMP|IR). P(CR|IR).P(CR)

The values for this scenario are shown in Table 4.37 since many incidents cause cybersecurity risk, and the combined probability assignment values for these incidents are more than 10%. The probability values are low when combining two combined probability assignments of cybersecurity risk. Thus, the calculations are performed using one combined incident, as Table 4.38 presents.

Table 4.37 Probability of Implementation Phase Risk Scenario 2

P(CR|IR) = 0.54166		
P(IMP|IR) = 0.23532		
(U) = Combined incidents 1 ∩ Combined incidents 2	P(CR|U)	P (CR, IR, IMP)
CR Due to AC, AD	0.20300	0.02558
CR Due to AE, AF	0.36756	0.04643
CR Due to BF, CC	0.20454	0.02578
CR Due to CF, DD	0.25314	0.03192
CR Due to DE, DF	0.36756	0.04643
CR Due to AB, AD	0.18706	0.02357

The highest implementation phase risk probability occurs when cybersecurity probability is calculated using one combined incident, as follows: when cybersecurity risk happens due to cyber-attacks (Component F) when combined with lack of maintenance of model for systems (Component A), or with lack of integration and interoperability between systems (Component B), or with improper security updates (Component C), or with lack of security awareness (Component D), or with IoT devices vulnerability (Component E) with a value of 0.12274.

Table 4.38 Probability of Implementation Phase Risk Scenario 2, Using One Combined Incident.

P(CR|IR) = 0.54166		
P(IMP|IR) = 0.23532		
Combined incident	P(CR| Combined Incidents)	P (CR, IR, IMP)
CR Due to AC	0.47183	0.05969
CR Due to AD	0.48837	0.06180
CR Due to AE	0.38577	0.04874
CR Due to AF	0.96346	0.12274
CR Due to BF	0.87714	0.11161
CR Due to CC	0.24401	0.03077
CR Due to CF	0.96466	0.12290
CR Due to DD	0.26582	0.03353
CR Due to DE	0.38577	0.04874
CR Due to DF	0.96346	0.12274
CR Due to EF	0.97064	0.12367
CR Due to FF	0.97183	0.12382

The third scenario for implementation phase risk is to occur due to network infrastructure risk (NR), which may result from cybersecurity risk (CR). The cybersecurity risk probability is calculated using Bayesian theory (3.10). Since cybersecurity risk occurs due to multiple combined incidents, the values of implementation risk probabilities are presented in Table 4.39 because the combined probability assignments for incidents causing cybersecurity risk are high.

The graphical presentation is provided in Figure 4.12.

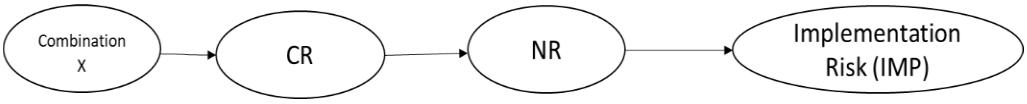


Figure 4.12 Implementation Phase Risk Scenario 3

The probability of this scenario is calculated using the equation 3.14 as :

P (CR, NR, IMP) = P(IMP|NR). P(CR|NR).P(CR)

Table 4.39: Probability of Implementation Risk Scenario 3

P(CR|NR) = 0.3043		
P(IMP|NR) = 0.11114		
Combined incident	P(CR| Combined Incidents)	P (CR, NR, IMP)
CR Due to AC	0.47183	0.01595
CR Due to AD	0.48837	0.01651
CR Due to AE	0.38577	0.01304
CR Due to AF	0.96346	0.03257
CR Due to BF	0.87714	0.02965
CR Due to CC	0.24401	0.00825
CR Due to CF	0.96466	0.03261
CR Due to DD	0.26582	0.00899
CR Due to DE	0.38577	0.01304
CR Due to DF	0.96346	0.03257

P(CR|NR) = 0.3043		
CR Due to EF	0.97064	0.03282
CR Due to FF	0.97183	0.03286

The probability of the third scenario is low because the probability of network infrastructure risk (NR) occurring is low, although the occurrence of cybersecurity risk is high.

The fourth scenario for the implementation phase risk to occur is due to integration risk (IR), which may result from the cascading effect of laws, regulations, and standards risk (LR), as presented graphically in Figure 4.13. The probability of this scenario is calculated using equation 3.14:

$P\ (LR, IR, IMP) = P(IMP|IR).\ P(LR|IR).P(LR) = 0.01124$

The laws, regulations, and standards risk (LR) probability is calculated using Bayesian theory (3.10), using the combined probability assignment of (Component R), the lack of application of policies, regulations, and standards, and (Component S), the lack of knowledge of policies, regulations, and standards, since it the has the maximum value, considering the worst-case scenario. Table 4.40 below summarizes the values used to calculate the probability of the fourth scenario.

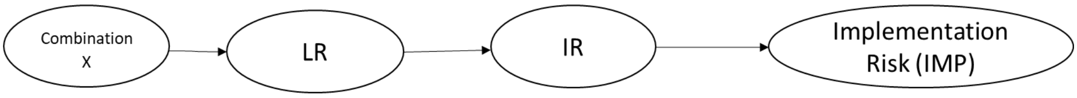


Figure 4.13 Implementation Phase Risk Scenario 4

Table 4.40: Summary of probabilities used to calculate implementation phase risk scenario 4

Probability	Value	Source
P(IMP|IR)	0.23532	Maximum value of this risk (Table 4.36)
P(LR|IR)	0.2	Calculated statistically from the data.
P(LR)	0.23883	This is calculated as P(LR| RS) using equation (3.10)

The fifth scenario causing implementation phase risk is resulting from the cascaded effect of financial risk (FR) that will cause resource and resource management risk (RMR), causing integration risk (IR) that will result in implementation phase risk. The scenario is graphically presented in Figure 4.14.

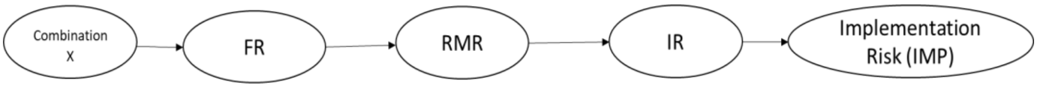


Figure 4.14 Implementation Phase Risk Scenario 5

The probability of this scenario is calculated using equation (3.14):

P (FR, RMR, IR, IMP) = P(IMP|IR). P(IR|RMR). P(RMR|FR).P(FR) =0.00479

The financial risk (FR) probability is calculated using Bayes theory (3.10), where the incident of the fear of capital cost (Component W) has the highest combined basic probability assignment. Table 4.41 below summarizes the values used to calculate the probability of the fourth scenario.

Table 4.41. Summary Of Probabilities Used to Calculate Implementation Phase Risk Scenario 5

Probability	Value	Source
P(IMP|IR)	0.23532	Maximum value of this risk (Table 4.34)
P(IR|RMR)	0.39285	Calculated statistically from the data.
P(RMR|FR)	0.35714	Calculated statistically from the data.
P(FR)	0.14533	This is calculated as P(FR| WW) using equation (3.10)

This scenario's probability is low compared to the other scenarios. Accordingly, the most significant probabilities are the probabilities of the implementation phase risk occurring due to the second and third scenarios.

4.4.3.4 Smart City Operation Phase Risks' Scenarios

The operation phase risk resulted from seven risks, namely cybersecurity risk (CR), technical data and applications risk (TR), network infrastructure risk (NR), integration risk (IR), data security and privacy risk (DR), stakeholder engagement risks(SER), and resource and resource management risks (RMR). The graphical presentation of the relationship for this scenario, scenario one, is presented in Figure 4.15

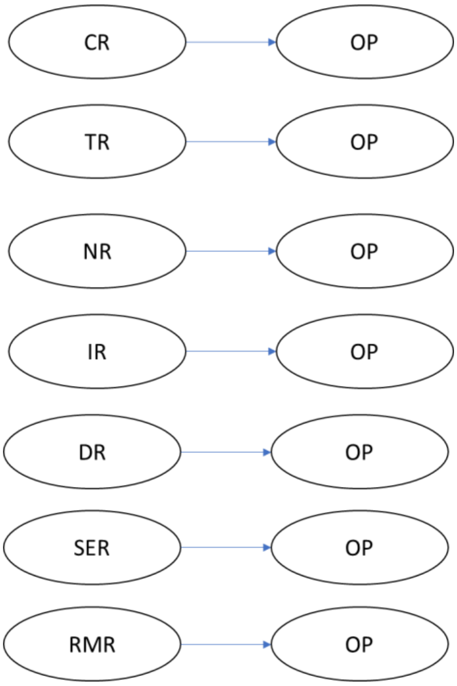


Figure 4.15 Operation Phase Risk Scenario1

The joint probability of this scenario is calculated, considering the combination of incidents causing each risk, where combinations with a value less than 10% are not considered since the values will be negligible.

The formula of Bayesian theory and joint probability (3.14) is used, and the marginal probability of operation phase risk occurring is calculated by counting the number of experts who mentioned any of the risks causing operation phase risk.

Table 4.42 represents the probabilities of Operation phase risk occurrence due to scenario 1.

Table 4.42.Operation Phase Risk Scenario 1 Probabilities.

Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(CR|U)	P(OP|CR)
CR	CR Due to AC, AD	0.20300	0.21723
	CR Due to AE, AF	0.36756	0.38771
	CR Due to BF, CC	0.20454	0.21885
	CR Due to CF, DD	0.25315	0.26970
	CR Due to DE, DF	0.36756	0.38771
	CR Due to AB, AD	0.18707	0.20046
	CR Due to EF, FF	0.94291	0.94735
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(TR|U)	P(OP|TR)
TR	TR Due to BD, DD	0.01090	0.01187
	TR Due to GB, GD	0.00971	0.01057
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(NR|U)	P(OP|NR)
NR	NR Due to BG, BD	0.02424	0.02636
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(IR|U)	P(OP|CR)
IR	IR Due to BB, BI	0.01840	0.02002
	IR Due to BJ, II	0.03010	0.03271
	IR Due to IJ, JJ	0.04222	0.04583
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(DR|U)	P(OP|DR)
DR	DR Due to DD, FD	0.13434	0.14463
	DR Due to FF, GD	0.21613	0.23101
	DR Due to GF	0.76650	0.78150
Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(SER|U)	P(OP|SER)
SER	SER Due to OO, OP	0.04554	0.04942
	SER Due to OQ, PP	0.02057	0.02237
	SER Due to PQ, QQ	0.05814	0.06301

Risk	(U) = Combined incidents 1 ∩ Combined incidents 2	P(RMR|U)	P(OP|RMR)
RMR	RMR Due to IV	0.20495	0.21928

To calculate the joint probability of the operation phase risk to occur due to CR, TR, NR, IR, DR, SER, and RMR, the maximum probability of operation phase risk to occur due to each risk is used, considering the worst-case scenario. Accordingly, the probability of planning phase risk due to CR, TR, NR, IR, DR, SER, and RMR is calculated using equation 3.14 as very low ≈0.00000014666.

The joint probability is calculated, considering that one combined incident causes each risk, and the combination of the highest value is used considering worst-case occurrence; thus, the value is calculated as 0.000063627. Table 4.43 presents the probabilities for each case.

Table 4.43. Operation Phase Risk Scenario 1 Probabilities Considering One Combined Incident.

Risk	Risk Due to Combined Incidents	P(CR| Combined Incidents)	P (OP|CR)
CR	CR Due to AC	0.47183	0.49324
	CR Due to AD	0.48837	0.50981
	CR Due to AE	0.38577	0.40629
	CR Due to AF	0.96346	0.96636
	CR Due to BF	0.87715	0.88609
	CR Due to CC	0.24401	0.26018
	CR Due to CF	0.96466	0.96747
	CR Due to DD	0.26582	0.28289
	CR Due to DE	0.38577	0.40629

	CR Due to DF	0.96346	0.96636
Risk	Risk Due to Combined Incidents	P(CR| Combined Incidents)	P (OP|CR)
	CR Due to AB	0.43810	0.45931
	CR Due to AD	0.48837	0.50981
	CR Due to EF	0.97064	0.97298
	CR Due to FF	0.97183	0.97408
Risk	Risk Due to Combined Incidents	P(TR| Combined Incidents)	P (OP|TR)
TR	TR Due to BD	0.08628	0.09328
	TR Due to DD	0.06465	0.07004
	TR Due to GB	0.05084	0.05515
	TR Due to GD	0.09753	0.10534
Risk	Risk Due to Combined Incidents	P(NR| Combined Incidents)	P (OP|NR)
NR	NR Due to BG	0.11114	0.119908
	NR Due to BD	0.11114	0.119908
Risk	Risk Due to Combined Incidents	P(DR| Combined Incidents)	P (OP|DR)
DR	DR Due to DD	0.152795	0.16423
	DR Due to FD	0.869978	0.879376
	DR Due to FF	0.942149	0.94665
	DR Due to GD	0.228421	0.243888
	DR Due to GF	0.7665	0.781499
Risk	Risk Due to Combined Incidents	P(DR| Combined Incidents)	P (OP|IR)
IR	IR Due to BB	0.072693	0.078691
	IR Due to BI	0.17577	0.188542
	IR Due to BJ	0.259645	0.276469
	IR Due to II	0.084507	0.091383
	IR Due to IJ	0.237899	0.253796

	IR Due to JJ	0.130435	0.140475
Risk	Risk Due to Combined Incidents	P(RMR| Combined Incidents)	P (OP|IR)
RMR	RMR Due to IV	0.204955	0.219284
Risk	Risk Due to Combined Incidents	P(SER| Combined Incidents)	P (OP|SER)
SER	SER Due to OO	0.178306	0.19122
	SER Due to OP	0.346808	0.366483
	SER Due to OQ	0.368349	0.38852
	SER Due to PP	0.077519	0.083879
	SER Due to PQ	0.354691	0.374557
	SER Due to QQ	0.218978	0.233999

The second scenario consideration for operation phase risk Figure 4.16 is caused by cybersecurity risk (CR) that will cause data security and privacy risks resulting in operation phase risk.

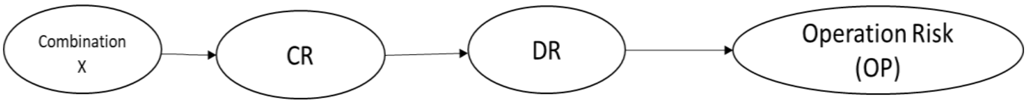


Figure 4.16: Operation Phase Risk Scenario 2

The probability of this scenario is calculated using equation (3.14) and denoted as :

P (CR, DR, OP) = P(OP|DR). P(DR|CR).P(CR)

The values for this scenario are shown in Table 4.44 since many incidents cause cybersecurity risk, and the values of combined probability assignment for these incidents are more than 10%. Considering the worst-case scenario, P(OP|DR) will use the maximum probability value.

Table 4.44 Probability of Operation Phase Risk Scenario 2

P(DR|CR) = 0.54166		
P(OP|DR) = 0.78150 (Table 4.42)		
(U) = Combined incidents 1 ∩ Combined incidents 2	**P(CR|U)**	**P (CR, DR, OP)**
CR Due to AC, AD	0.20300	0.085931
CR Due to AE, AF	0.36756	0.155591
(U) = Combined incidents 1 ∩ Combined incidents 2	**P(CR|U)**	**P (CR, DR, OP)**
CR Due to BF, CC	0.20454	0.086583
CR Due to CF, DD	0.25315	0.10716
CR Due to DE, DF	0.36756	0.155591
CR Due to AB, AD	0.18707	0.079188
CR Due to EF, FF	0.94291	0.399141

The highest probability of operation phase risk occurs when cybersecurity risk happens due to cyber-attacks (Component F) combined with IoT device vulnerability (Component E) with a value of 0.399141.

The probabilities of the second scenario are calculated using one combined incident for cybersecurity risk, considering the highest value of P(OP|DR) to calculate the worst-case scenario. The values are considerably high when cybersecurity risk happens due to cyber-attacks (Component F) combined with a lack of maintenance model for systems (Component A), lack of integration and interoperability between systems (Component B), improper security updates (Component C) lack of security awareness (Component D), and IoT devices vulnerability (Component E). Table 4.45 below will provide the calculated probabilities.

Table 4.45 Probability of Operation Phase Risk Scenario 2, using one combined incident.

P(DR|CR) = 0.54166	Calculated statistically	
P(OP|DR) = 0.94665 Table (4.41)		
Combined incident	P(CR| Combined incidents)	P(CR,DR, OP)
CR Due to AC	0.49324	0.25291
CR Due to AD	0.50981	0.26141
CR Due to AE	0.40629	0.20833
Combined incident	P(CR| Combined incidents)	P(CR,DR, OP)
CR Due to AF	0.96636	0.49551
CR Due to BF	0.88609	0.45435
CR Due to CC	0.26018	0.13341
CR Due to CF	0.96747	0.49608
CR Due to DD	0.28289	0.14505
CR Due to DE	0.40629	0.20833
CR Due to DF	0.96636	0.49551
CR Due to AB	0.45931	0.23551
CR Due to AD	0.50981	0.26141
CR Due to EF	0.97298	0.49891
CR Due to FF	0.97408	0.49947

The third scenario for operation phase risk is due to network infrastructure risk (NR), which may result from cybersecurity risk (CR). The cybersecurity risk probability is calculated using Bayesian theory (3.10). Since cybersecurity risk occurs due to multiple combined incidents, the values of operation risk probabilities are presented in Table

4.46. The calculations will consider one combined incident causing cybersecurity risk to reflect worst-case scenarios. The graphical presentation is provided in Figure 4.17

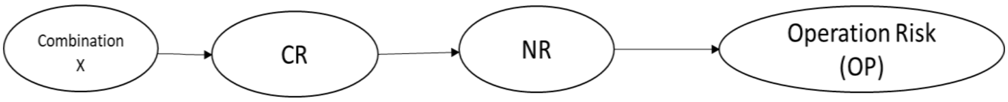


Figure 4.17 Operation Phase Risk Scenario 3

The probability of this scenario is calculated using the equation 3.14 as :

P (CR, NR, OP) = P(OP|NR). P(NR|CR).P(CR)

Table 4.46. Probability of Operation Risk Scenario 3

P(NR|CR) = 0.3043	Calculated statistically from the data	
P(OP|NR) = 0.119908 Table (4.43)		
Combined incident	P(CR| Combined Incidents)	P (CR, NR, OP)
CR Due to AC	0.49325	0.01800
CR Due to AD	0.50981	0.01860
CR Due to AE	0.40629	0.01482
CR Due to AF	0.96637	0.03526
CR Due to BF	0.88610	0.03233
CR Due to CC	0.26019	0.00949
CR Due to CF	0.96747	0.03530
CR Due to DD	0.28289	0.01032
CR Due to DE	0.40629	0.01482
CR Due to DF	0.96637	0.03526
CR Due to AB	0.45932	0.01676
CR Due to AD	0.50981	0.01860
CR Due to EF	0.97299	0.03550
CR Due to FF	0.97409	0.03554

The probability of the third scenario is low because the probability of network infrastructure risk (NR) occurring is low, although the probability of occurrence of cybersecurity risk is high.

The fourth scenario for operation phase risk to occur is due to the occurrence of integration risk (IR), which may result from the cascading effect of resources and resource management risk (RMR), as presented graphically in Figure 4.18. The probability of this scenario is calculated using equation 3.14:

P (RMR, IR, OP) = P(OP|IR). P(IR|RMR).P(RMR) = 0.02226

The resources and resource management risk (RMR) probability is calculated using Bayes theory (3.10), using the combined probability assignment of (Component I), the limited knowledgeable human resources, and (Component V) the lack of budget, since it the has the maximum value, considering the worst-case scenario. Table 4.47 below summarizes the values of this scenario.

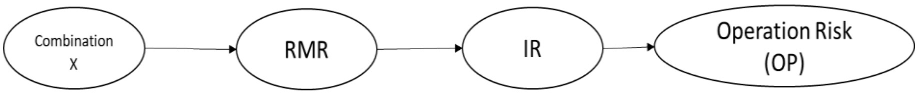


Figure 4.18 Operation Phase Risk Scenario 4

Table 4.47: Summary of Probabilities Used to Calculate Operation Phase Risk Scenario 4

Probability	Value	Source
P(OP|IR)	0.2764	Maximum value of this risk (Table 4.41)
P(IR|RMR)	0.3929	Calculated statistically from the data.
P(RMR)	0.20495	This is calculated as P(RMR| IV) using equation (3.10)

The value of this scenario is low in comparison with the second scenario.

The fifth scenario causing operation phase risk is resulting from the cascaded effect of cybersecurity risk (CR), which will cause technical data and applications risk (TR) in operation phase risk. The scenario is graphically presented in Figure 4.19.

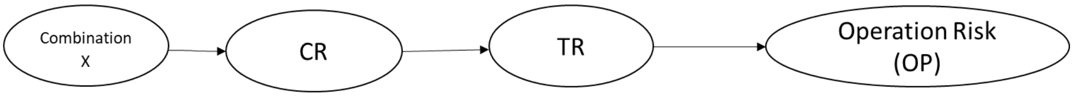


Figure 4.19: Operation Phase Risk Scenario 5

The probability of this scenario is calculated using equation 3.14:

P (CR, TR, OP) = P(OP|TR). P(TR|CR). P(CR)

The cybersecurity risk (CR) probability is calculated using Bayesian theory (3.10), considering one combined incident. The basic probability assignments for combined incidents causing cybersecurity risk are above 10%. Thus, the cases in this scenario are presented in Table 4.48.

Table 4.48: Summary Of Probabilities Used To Calculate Operation Phase Risk Scenario 5.

P(TR|CR) = Calculated statistically from the data		
P(OP|TR) = 0.10534 Table (4.41)		
Combined incident	P(CR| Combined Incidents)	P (CR, TR, OP)
CR Due to AC	0.49325	0.017320
CR Due to AD	0.50981	0.017901
CR Due to AE	0.40629	0.014266
CR Due to AF	0.96637	0.033932
CR Due to BF	0.88610	0.031114
CR Due to CC	0.26019	0.009136
CR Due to CF	0.96747	0.033971
CR Due to DD	0.28289	0.009933
CR Due to DE	0.40629	0.014266
CR Due to DF	0.96637	0.033932
CR Due to AB	0.45932	0.016128
CR Due to AD	0.50981	0.017901
CR Due to EF	0.97299	0.034165
CR Due to FF	0.97409	0.034204

The probability of this scenario to occur is low compared to the other scenarios. Accordingly, the most significant probability of operation phase risk is when this risk occurs due to the second scenario.

The previous section provided the risk and incidents graphical model outcome of Phase 2 of the suggested framework Figure 3.1. Also, this section provided the calculation using the risk assessment tool to calculate risk probabilities by combining Dempster Shafter theory and Bayesian Joint probability.

4.4.3.5 Evaluation Criteria using AHP.

The analytical hierarchy process is used to develop the evaluation criteria based on Gioia results Figure 4.1, to evaluate the risk scenario probabilities. As per the resulting grounded theory provided in section 4.4.1, The main goal is to ensure smart city sustainability through proper risk management. As per the defined steps of AHP, the problem is defined in the following chart illustrated in Figure 4.20

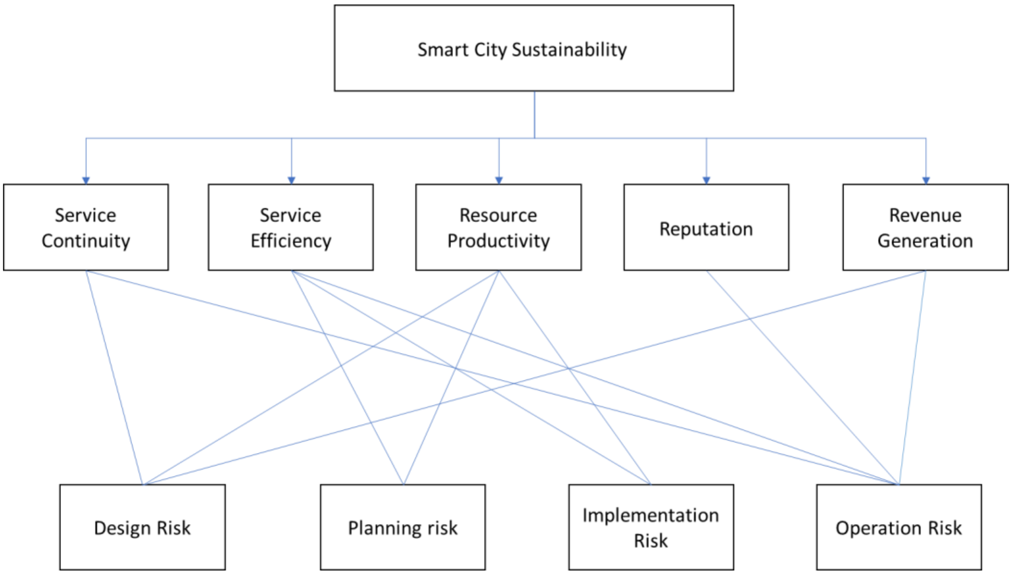


Figure 4.20 AHP Problem Definition.

To achieve smart city sustainability through proper risk assessment. Five criteria are defined based on the discussions with experts: service continuity, service efficiency, resource productivity, reputation, and revenue generation. The second level illustrates the project's phase risks resulting from the identified risks' scenarios in section 4.4.3.

A pair-wise comparison matrix between the five impacts affecting smart city sustainability is constructed based on the experts' views and a focus group meeting, resulting in the ratings used in the pair-wise matrix. The used scale is suggested by(

Saaty, 1987). Table 4.49 represents the ratings of the five criteria used in the study. The normalized matrix and the criteria weights are presented in Table 4.50. The Consistency ratio is calculated using equation 3.16, and it shows a value of 0.0316, which is acceptable for a criteria matrix with n= 5 (Saaty, 1987).

Table 4.49: Pair-Wise Comparison Matrix.

	Service Continuity	Service Efficiency	Resource Productivity	Reputation	Revenue Generation
Service Continuity	1.00	1.00	3.00	7.00	9.00
Service efficiency	1.00	1.00	2.00	8.00	7.00
Resource productivity	0.33	0.50	1.00	2.00	5.00
Reputation	0.14	0.13	0.50	1.00	3.00
Revenue Generation	0.11	0.14	0.20	0.33	1.00

Table 4.50: Normalized Pair-Wise Comparison Matrix.

	Service Continuity	Service Efficiency	Resource Productivity	Reputation	Revenue Generation	Criteria Weights
Service Continuit	0.39	0.36	0.45	0.38	0.36	0.39
Service Efficiency	0.39	0.36	0.30	0.44	0.28	0.35
Resource productivi	0.13	0.18	0.15	0.11	0.20	0.15
Reputation	0.06	0.05	0.07	0.05	0.12	0.07
Revenue Generation	0.04	0.05	0.03	0.02	0.04	0.04

According to the results, the weight of service continuity is 0.39, which indicates the importance of having continuous services in a smart city project. The service efficiency is high at 0.35, which is crucial for sustainable smart city projects. Resource productivity is of moderate importance, but resource productivity will affect service continuity and efficiency. The lower values are given to reputation and revenue generation, which will be affected by service continuity and productivity.

To construct the decision matrix, a pair-wise matrix is constructed for each smart city project phase risk with each criterion as follows:

The service Continuity matrix is constructed in Table 4.51, and consistency is tested using equation 3.16. and it has a value of 0.05914, which is accepted since the matrix four criteria matrix.

Table 4.51 Pair-wise Comparison Matrix for Service Continuity SC-Project Phase Risk

	DES	PLAN	IMP	OP
Design Phase Risk (DES)	1.00	5.00	8.00	9.00
Planning Phase Risk (PLAN)	0.20	1.00	2.00	6.00
Implementation Phase Risk (IMP)	0.13	0.50	1.00	3.00
Operation Phase Risk (OP)	0.11	0.17	0.33	1.00

The normalized matrix and the weights are the results, as presented in Table 4.52.

Table 4.52 Pair-Wise Normalized Comparison Matrix For Service Continuity And SC-Project Phase Risk

	DES	PLAN	IMP	OP	Criteria Weights
Design Phase Risk (DES)	0.70	0.75	0.71	0.47	0.66
Planning Phase Risk (PLAN)	0.14	0.15	0.18	0.32	0.20
Implementation Phase Risk (IMP)	0.09	0.08	0.09	0.16	0.10
Operation Phase Risk (OP)	0.08	0.03	0.03	0.05	0.05

The service efficiency matrix is built as Table 4.53 presents, the consistency index is calculated, and it has a value of 0.021572.

Table 4.53 Pair-Wise Comparison Matrix For Service Efficiency And SC-Project

Phase Risk

	DES	PLAN	IMP	OP
Design Phase Risk (DES)	1.00	0.11	0.13	0.25
Planning Phase Risk (PLAN)	9.00	1.00	0.50	2.00
Implementation Phase Risk (IMP)	8.00	2.00	1.00	3.00
Operation Phase Risk (OP)	4.00	0.50	0.33	1.00

The normalized matrix and the criteria weights are presented in Table 4.54.

Table 4.54. Normalized Matrix for Service Efficiency And SC-Project Phase

	DES	PLAN	IMP	OP	Criteria Weights
Design Phase Risk (DES)	0.05	0.03	0.06	0.04	0.05
Planning Phase Risk (PLAN)	0.41	0.28	0.26	0.32	0.32
Implementation Phase Risk (IMP)	0.36	0.55	0.51	0.48	0.48
Operation Phase Risk (OP)	0.18	0.14	0.17	0.16	0.16

The resource productivity matrix is built as Table 4.55 presents, the consistency index is calculated, and it has a value of 0.012664776.

Table 4.55 Pair-Wise Comparison Matrix For Resource Productivity And SC-Project Phase Risk

	DES	PLAN	IMP	OP
Design Phase Risk (DES)	1.00	0.11	0.33	1.00
Planning Phase Risk (PLAN)	9.00	1.00	2.00	5.00
Implementation Phase Risk (IMP)	3.00	0.50	1.00	3.00
Operation Phase Risk (OP)	1.00	0.20	0.33	1.00

The normalized matrix and the criteria weights are presented in Table 4.56.

Table 4.56 The Normalized Matrix for Resource Productivity and SC Project Phase

	DES	PLAN	IMP	OP	Criteria Weights
Design Phase Risk (DES)	0.07	0.06	0.09	0.10	0.08
Planning Phase Risk (PLAN)	0.64	0.55	0.55	0.50	0.56
Implementation Phase Risk (IMP)	0.21	0.28	0.27	0.30	0.27
Operation Phase Risk (OP)	0.07	0.11	0.09	0.10	0.09

The reputation matrix is built as per Table 4.57, and the consistency index is calculated at 0.023289655.

Table 4.57: The Pair-Wise Comparison Matrix for Reputation and SC Project Phase

	DES	PLAN	IMP	OP
Design Phase Risk (DES)	1.00	0.50	0.25	0.11
Planning Phase Risk (PLAN)	2.00	1.00	0.33	0.13
Implementation Phase Risk (IMP)	4.00	3.00	1.00	0.25
Operation Phase Risk (OP)	9.00	8.00	4.00	1.00

The normalized matrix and the criteria weights are presented in Table 4.58

Table 4.58: The Normalized Matrix for Reputation and SC Project Phase

	DES	PLAN	IMP	OP	Criteria Weights
Design Phase Risk (DES)	0.06	0.04	0.04	0.07	0.06
Planning Phase Risk (PLAN)	0.13	0.08	0.06	0.08	0.09
Implementation Phase Risk (IMP)	0.25	0.24	0.18	0.17	0.21
Operation Phase Risk (OP)	0.56	0.64	0.72	0.67	0.65

The revenue generation matrix is built as per Table 4.59, where the consistency index is calculated and has a value of 0.022626867.

Table 4.59: The Pair-Wise Comparison Matrix for Revenue Generation and SC Project Phase Risk.

	DES	PLAN	IMP	OP
Design Phase Risk (DES)	1.00	2.00	2.00	0.25
Planning Phase Risk (PLAN)	0.50	1.00	0.50	0.13
Implementation Phase Risk (IMP)	0.50	2.00	1.00	0.25
Operation Phase Risk (OP)	4.00	8.00	4.00	1.00

The normalized matrix and the criteria weights are presented in Table 4.60

Table 4.60: The Normalized Comparison Matrix For Revenue Generation And SC-Project Phase Risk.

	DES	PLAN	IMP	OP	Criteria Weights
Design Phase Risk (DES)	0.17	0.15	0.27	0.15	0.19
Planning Phase Risk (PLAN)	0.08	0.08	0.07	0.08	0.08
Implementation Phase Risk (IMP)	0.08	0.15	0.13	0.15	0.13
Operation Phase Risk (OP)	0.67	0.62	0.53	0.62	0.61

The resulting evaluation criteria matrix based on the previous calculations is shown in Table 4.61 below. The evaluation criteria provide each smart city phase risk level's impact on service continuity, efficiency, resource productivity, reputation, and revenue generation. For example, the impact of design phase risk (DES) concerning service continuity is 0.65647, and the impact of planning phase risk (PLAN) concerning service efficiency is 0.31533. In addition, the importance of the pillars concerning smart city sustainability is calculated, so the importance of service continuity concerning smart city sustainability is 0.38747. Smart city decision-makers may use the resulting criteria during any project’s phase to assess risks and scenarios and take the proper countermeasures to ensure smart city sustainability. The matrix allows for the prioritization of risks based on the specified criteria. The evaluation criteria are the outcome of Phase 3 of the suggested Framework in Figure 3.1

Table 4.61: Risk Evaluation Criteria.

	Service Continuity (0.38747)	Service efficiency. (0.35253)	Resource productivity (0.15356)	Reputation (0.06991)	Revenue Generation (0.03652)
Design Phase Risk (DES)	0.65647	0.04501	0.08092	0.05551	0.18526
Planning Phase Risk (PLAN)	0.19538	0.31533	0.56011	0.08720	0.07596
Implementation Phase Risk (IMP)	0.10204	0.47703	0.26577	0.20933	0.13109
Operation Phase Risk (OP)	0.04610	0.16262	0.09319	0.64795	0.60769

According to the resulting evaluation criteria, the scenarios of risks are evaluated using the weighted sum equation (3.17). The design risk total impact on the smart city project is 0.29330. Accordingly, if scenario 3 occurred, for instance, the value of design risk will be calculated as the probability of this scenario to occur multiplied by the impact of design risk, which will equal to 0.02532.

The planning risk total impact is 0.28175. Therefore, the value of the planning risk if scenario 3 occurred, for example, equals 0.03064. The total impact of the implementation risk is calculated as 0.26794. Then, the value of implementation risk, for instance, will be 0.03288 if scenario 2 occurs. The operation risk total impact is computed as 0.15699. Thus, the value of operation risk equals 0.0784 if scenario 2 occurred, for instance.

Management can use these values to make informative and precise decisions when analyzing risks.

4.5 Framework Evaluation

The framework is evaluated using a focus group with fifteen smart city experts. During the focus group meeting, the outcome of each phase is discussed and explained, and then the system usability score SUS (Brooke, 2020) is discussed and sent to the participants after the meeting. The results of the framework evaluation process are discussed as follows.

4.5.1 Focus Group Evaluation

The focus group comprises fifteen experts who worked on smart city projects during different phases. Four members are from the management level, two are experts in designing and planning, and nine worked in the implementation and operation phases. The outputs of each phase of the risk assessment framework are discussed. For the resulting grounded theory, management-level experts acknowledged the five pillars, service continuity, service efficiency, resource productivity, reputation, and revenue generation, that will affect smart city sustainability; the risk assessment framework will consider risks' impact on these pillars and the average SUS score of .78.6%, which acceptable evaluation since it is above 50% as mentioned by (Calciolari et al., 2022) when evaluating a similar conceptual framework.

The graphical presentation of risk scenarios and the causal relations between risks are illustrated. The designing and planning experts accepted the proposed scenarios as the major scenarios that may occur, including resulting relationships between risks. The implementation and operation experts admitted the resulting scenarios with the SUS score value of 80.4% and suggested having detailed guidelines to apply the framework in the industry. The evaluation criteria are presented and discussed during the focus group, and the responses agree with the achieved percentages and weights of the criteria with an SUS score of 78.7%.

4.5.2 System Usability Scale Evaluation

The SUS questionnaire developed and discussed by (Brooke, 2020) is distributed to the fifteen experts who worked on smart city projects regionally and internationally to test the framework's usability. The System Usability Scale SUS evaluation is performed on each framework's phase output. Table 4.62 evaluates Phase 1 outcomes and the resulting grounded theory from initial data analysis. The evaluation contains questions about the consistency of the theory, its usage, and its level of complexity. (The SUS evaluation questionnaire is available in APPENDIX B.) The average score is 78.68, which is acceptable per the defined average SUS score of 68 (Lewis & Sauro, 2018). When analyzing individual scores, all experts provided scores above 50.

Table 4.62.SUS score for Phase 1: Initial Data Analysis output

Expert	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS Score
1	5	2	3	3	4	2	4	2	4	2	72.5
2	4	1	4	2	5	1	4	2	5	1	87.5
3	2	2	4	1	5	1	5	2	5	1	85
4	5	1	5	1	5	1	5	1	5	1	100
5	4	2	4	1	3	1	5	1	4	2	82.5
6	3	2	3	4	3	1	5	3	2	5	52.5
7	4	1	4	3	4	1	4	1	4	2	80
8	5	1	5	1	5	1	5	1	5	1	100
9	5	1	4	2	5	1	5	1	5	1	95
10	3	3	3	4	5	2	3	3	3	2	57.5

Expert	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS Score
11	4	1	3	1	4	1	3	1	4	2	80
12	4	1	4	5	4	1	5	1	4	2	77.5
13	4	1	4	5	4	1	4	1	4	1	77.5
14	4	3	4	2	3	3	4	3	4	3	62.5
15	4	2	3	2	3	1	4	2	3	2	70.0

The interrelations between risks, presented in section 4.4.4 and the graphical presentation of these relations, are evaluated, where each smart city project phase risk scenarios are evaluated in terms of consistency of the relationship between risks and the usability of these scenarios to smart city management. The following tables present the SUS evaluation scores for design and planning phase risk scenarios, Table 4.63; implementation phase risk scenarios, Table 4.64; and operation phase risk scenarios, table 4.65. The scores have an average of 80.33.,79.5,81.33, respectively, which are accepted. The individual scores given by each expert are between 60 and 100. Thus, the evaluation is accepted per the rates mentioned (Lewis & Sauro, 2018).

Table 4.63 SUS score for Phase 2: Design and Planning Phases Risk Scenarios

Expert	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS Score
1	4	1	3	3	4	2	4	2	4	3	70
2	5	2	4	2	5	2	4	1	4	2	82.5
3	5	2	5	1	5	1	5	1	5	1	97.5
4	5	1	5	1	5	1	5	1	5	1	100
5	5	1	4	2	3	1	5	1	4	2	85
6	5	1	4	4	4	1	4	1	5	3	80
7	4	1	4	3	4	1	3	1	4	1	80
8	5	1	5	1	5	1	5	1	5	1	100
9	5	1	5	1	5	1	5	1	5	1	100
10	4	2	2	3	4	2	4	3	3	2	62.5
11	4	1	4	1	3	2	3	1	4	2	77.5
12	4	2	3	5	4	1	3	2	3	3	60
13	5	1	4	5	5	1	5	1	5	1	87.5
14	4	2	3	2	3	3	3	2	4	2	65.0
15	4	1	3	2	3	1	4	2	3	2	72.5

Table 4.64 SUS score for Phase 2: Implementation Phase Risk Scenarios

Expert	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS Score
1	4	2	3	3	4	2	4	1	3	2	70
2	5	2	4	2	4	1	4	1	4	2	82.5
3	5	1	5	1	5	1	5	1	5	1	100
4	5	1	5	1	5	1	5	1	5	1	100
5	5	1	4	2	3	1	5	1	4	1	87.5
6	5	2	3	4	2	4	2	2	3	3	50

Expert	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS Score
7	4	1	4	3	4	1	3	1	4	2	77.5
8	5	1	5	1	5	1	5	1	5	1	100
9	5	1	5	1	5	1	5	1	5	1	100
10	4	2	2	3	4	2	4	3	3	2	62.5
11	3	2	3	1	4	2	3	1	3	3	67.5
12	4	1	3	5	4	1	4	2	4	2	70
13	5	1	4	5	5	1	5	1	5	1	87.5
14	4	2	4	2	3	3	3	2	4	2	67.5
15	5	2	3	2	3	1	4	2	3	3	70.0

Table 4.65 SUS score for Phase 2: Operation Phase Risk Scenarios

Expert	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS Score
1	4	2	3	3	4	2	4	1	3	2	70
2	5	2	4	1	5	1	5	1	5	2	92.5
3	4	2	5	1	5	1	5	1	5	1	95
4	5	1	5	1	5	1	5	1	5	1	100
5	5	1	4	2	3	1	5	1	4	2	85
6	5	3	4	5	4	1	4	2	2	4	60
7	4	1	4	3	4	1	3	1	3	2	75
8	5	1	5	1	5	1	5	1	5	1	100
9	5	1	5	1	5	1	5	1	5	1	100
10	4	2	2	3	4	2	4	3	3	2	62.5
11	3	2	4	1	3	2	4	1	4	3	72.5
12	4	2	3	5	4	1	4	2	4	3	65
13	5	1	4	4	5	1	5	1	5	1	90.0

Expert	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS Score
14	3	2	3	2	3	2	3	2	3	2	62.5
15	4	1	4	2	3	1	4	2	3	2	75.0

In the evaluation of Phase 3, which contains the evaluation criteria, resulted in an average score of 78.67, and the usability criteria for smart city management and consistency were evaluated. The individual scores are presented in Table 4.66.

Table 4.66: SUS Score for Phase 3: Smart City Risks Evaluation Criteria

Expert	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS Score
1	4	2	3	3	4	2	4	2	4	2	70
2	4	2	4	2	5	1	5	1	5	2	87.5
3	4	4	4	4	3	1	4	4	2	3	52.5
4	5	1	5	1	5	1	5	1	5	1	100
5	5	1	4	2	4	1	5	1	4	1	90
6	4	1	4	3	4	1	5	2	4	3	77.5
7	4	1	4	3	3	1	4	1	4	1	80
8	5	1	5	1	5	1	5	1	5	1	100
9	5	1	5	1	5	1	5	1	5	1	100
10	3	3	3	3	4	2	3	2	3	2	60
11	3	2	4	3	4	2	3	2	4	2	67.5
12	4	2	3	5	4	1	4	2	4	3	65
13	5	1	4	5	5	1	5	1	5	1	87.5
14	4	1	4	1	3	3	3	2	4	2	72.5
15	4	2	3	2	3	1	4	2	3	2	70.0

4.6 Results Discussion

This section discusses the thesis findings and the research questions. The discussion aims to declare the achievement of the research objectives in the following paragraphs.

4.6.1 Analysis of RQ1

The first research question concerns the risk types applicable to smart city projects. Smart cities are generally considered an expression in many countries to indicate the use of technology for some of their governance processes. As mentioned in this thesis, multiple dimensions must be considered to obtain ‘smart’ outcomes for a city. Smart outcomes, however, need the right use of technology, governance processes, and participation from different sectors of society. However, technology, integration systems, and governance can invite technical and non-technical risks. Such risks may not be understood well by the planners, and it can lead to misperceptions of smart city applications and advantages.

The capability to design the smart city ecosystem and integrate it with a better risk management process can support the objective of a smart city. The study highlights the opportunities and risk-based challenges related to smart cities. The study presents technical and non-technical risks in smart city design, planning, implementation, and operation.

The literature focuses on technical risks because smart cities are usually understood in terms of using smart technologies and systems. Although very few researchers focus on non-technical risks, it is emphasized that addressing non-technical risks such as social, economic, governance, legal, and strategic risks can improve the outcomes of smart city design, planning, implementation, and operation.

Therefore, and as the results of this study present, the aspirants of smart city design and planning have to analyze non-technical threats, like management changes, hierarchy, planning, and organizational vision, to avoid strategic risk. Considering people’s mindsets of resisting change and using smart systems and the lack of communication between different stakeholders will support the identification of stakeholder engagement risks.

The awareness and application of policies, regulations, and standards are mandatory to avoid the risk of laws, regulations, and standards, especially during the early design phase. Smart city sustainability can be assured when considering a clear business continuity model and continuous data analysis, which will minimize business continuity risk.

Smart city designers and planners should pay attention to budget details and investments in smart city projects to avoid financial risk. The limited knowledge of human resources and experts in smart city design, planning implementation, and operation is a main challenge that causes resource and resource management risk. Early awareness of this risk from the design phase will enable decision-makers to take countermeasures to mitigate this risk.

Moreover, non-technical risks must be considered in addition to technical risks during implementation and operation. The main non-technical risks that should be considered are stakeholder engagement risk, laws, regulations, standards risk, financial risk, and resource and resource management risk. In addition, technical threats such as lack of maintenance model for systems, lack of Integration and interoperability between systems, improper security awareness and updates, IoT devices vulnerability, and cyber-attacks should be examined to prevent cybersecurity risk.

Smart city implementers and operators must consider the wrong operation and the mentioned technical threats to prevent technical data and applications risks, data security and privacy risks, and network infrastructure risks. The integration risk is a main risk to be anticipated by considering the limited knowledgeable human resources and experts, the limited integration and operability between systems and the usage of closed code programs.

In the previous paragraphs, the study illustrates that technical and non-technical risks are applicable in a smart city project.

4.6.2 Analysis of RQ2

The second research question concentrates on the interrelations between different types of risks. The interrelations between different types of risks are presented in the results, based on the interviews with experts and the correlation tests performed on the data.

Technical risks may occur due to a shared incident. For instance, cybersecurity, technical data, and application risks may occur due to a lack of Integration and interoperability between systems or security awareness. These incidents are correlated; cybersecurity and technical data and application risks are interrelated. Furthermore, cybersecurity risk, data security, and privacy risk have common incidents that are related with high correlation coefficients. These incidents are cyber-attacks and a lack of security awareness. The resulting interrelations are supported by other studies (Ismagilova et al., 2022).

Network infrastructure risk has common incidents with cybersecurity risk, including lack of Integration and interoperability between systems, lack of maintenance model for systems, and lack of security awareness. In addition, the risk shares wrong operation incidents with technical data and application risk. The common incidents are correlated; therefore, the risks are associated.

The integration risk has a common incident with cybersecurity, technical data and application, and network infrastructure risks. This incident is due to a lack of integration and interoperability between systems. Accordingly, these risks have interrelations.

The interview with smart city experts showed that technical risks are related to non-technical risks. This finding is supported by Shayan et al.,(2020), but the detailed relations are not identified in the study.

The results from phase 2 of the smart city risk assessment framework proposed in this study show that laws, regulations, and standards risk are related to integration risk, standards are crucial for integration between systems and hardware and software, and lack of awareness of regulations and standards will initiate integration risk. Also, resource and resource management risks that may be caused by limited knowledgeable human resources and experts will lead to integration risks.

The smart city experts highlighted the interrelations between non-technical risks. The financial risk is interrelated with resource and resource management risk, where a lack of budget will affect hiring knowledgeable resources and experts.

The change in management hierarchy and planning will cause strategic risk, leading to a lack of communication among different stakeholders and thus causing stakeholder engagement risk.

Also, the results illustrate that the lack of awareness and application of laws, regulations, policies, and standards will cause risks to laws, regulations, and standards, affecting business continuity planning and causing business continuity risk. The unclear continuity plans will lead stakeholders to fear investment in smart city projects, and thus, financial risk may be caused.

The literature highlighted that there are interrelations between risks, yet the authors recommended comprehensive studies to have a complete risk assessment method for smart cities (Techatassanasoontorn & Suo, 2010)

4.6.3 Analysis of RQ3

The third research question focuses on what should be integrated to develop a generic assessment framework for smart cities. A smart city project is complex and involves multiple disciplines, including urban planning, technology, social, and management sciences. Developing a generic risk assessment framework requires a comprehensive understanding of technical and non-technical risks for smart city projects. Understanding the incidents causing each risk is mandatory for comprehensive assessment, as the results of the first phase of the suggested framework illustrate.

The interrelations and interactions between risks must be identified, and the main risk scenarios for each smart city project phase, design, planning, implementation, and operation must be specified. Risk incident probabilities must be considered while calculating the joint probabilities of risk scenarios. The suggested framework's second phase output provides interrelations and joint probabilities calculations.

The impacts of the risks on smart city projects and city sustainability should be recognized. The impacts on smart city service continuity, efficiency, resource productivity, reputation, and revenue generation should be recognized. Then, evaluating risks compared to impacts is crucial for decision-makers to take the proper measures to mitigate risks. The evaluation is illustrated in the third phase of the suggested framework.

4.6.4 Analysis of RQ4

The fourth research question focuses on applying the suggested risk assessment framework to assess risk in a smart city design, planning, implementation, and operation.

Risk assessment, by definition, includes identifying, analyzing, and prioritizing potential risks a project may encounter. The suggested framework proposes a comprehensive method to identify, analyze, and prioritize risks a smart city project may face during different phases of the project.

Potential risks are identified through comprehensive interviews with smart city experts who have worked regionally and internationally. The experts are diverse, which allowed the identification of incidents causing risks and the main risks applied in smart city projects. The results are illustrated in Table (4.4). Smart city project teams could use the resulting list to identify the applicable incidents and risks within the project.

Analysis of incidents causing risks is performed using the Dempster-Shafer theory, where a combination of incidents and probabilities are identified to get the combined basic probability assignments. The values of the combined basic probabilities assignments provide indications of the critical incidents that the smart city project team needs to consider during the design, planning, implementation, and operation phases. Identified scenarios will provide an idea of the interrelations between risks. Accordingly, proper mitigation plans can be prepared.

The findings show that at the design phase, decision-makers must focus on strategic risk, stakeholder engagement risk, laws and regulations risk, business continuity risk, and financial risk. Attention to different technical risks is recommended. The results also indicate that the most probable scenario to occur causing design phase risk is the scenario that starts from strategic risk, leading to stakeholders' engagement risk and then the design risk, with a probability of 8%

Proper management of these risks will secure service continuity, increase resource productivity, and enhance future revenue generation.

Similarly, decision-makers must concentrate on strategic, stakeholder engagement, and financial risks in the planning phase since the most probable scenario to occur is starting with strategic risk, leading to stakeholders' engagement risk, and then planning risk with a probability of 10 %. Yet, resource and resource management risks must be paid proper attention to ensure productivity and efficiency. Thus, smart city decision-makers must have a clear vision for the smart city with a proper business model that will secure the sustainability and continuity of the city. Also, a stakeholder management plan needs to be in place to have stakeholders' acknowledgment and support for the smart city project. Financial planning is a major element to be considered to avoid over-budget and unnecessary costs that may occur.

Technology-related risks play a significant role in the implementation phase; smart city implementers must pay attention to cybersecurity, network infrastructure, and integration risks. The results denote that the highest probability of implementation phase risk results from cybersecurity risk, which leads to integration risk with a value of 12%.

In addition, stakeholder engagement and resource and resource management risks must be studied to confirm services' efficiency and enhance resource productivity.

Therefore, during the implementation phase, implementation experts must continuously refer to strategic plans and ensure robust communication between different stakeholders to expedite the implementation, especially with the complexity of a smart city project. Regarding technology alignment with laws, regulations, and standards, the implementation team must have rigorous knowledge of the country's legislation to avoid delays, additional costs, and reputation impacts.

From a technology perspective, integration between smart city applications and hardware devices must be considered in terms of integration experts, used technology, and scope of work, in addition to the full awareness of security measures, cyberattacks, network designs, and systems interoperability. Accordingly, the financial impacts of service interruption impact will be minimized.

Results give insights to smart city management and decision-makers during the operation phase. Smart city operators need to have proper information about the vision and mission of the smart city project, which will support the operation within the project's scope. Operation experts must regularly communicate with stakeholders, including higher management, to highlight any threats or incidents that may cause technical and non-technical risks. Stakeholder management has low consideration by the operation team; planning and implementation teams must communicate their view of risks to operational teams to ensure adequate risk identification and mitigation planning during operation. Mitigating these risks will ensure service continuity, productivity, and efficiency during operation, guarantee expenses within budget, and build a respectful reputation.

Proper resources must be acquired for each phase of the project to avoid risks from resource scarcity. Furthermore, preventative measures must be taken regarding technical risks, such as identifying the technology to be used and ensuring that the used technology and equipment align with the country’s laws and standards. Besides, cybersecurity measures, data security and privacy procedures, and proper network designs are crucial; the results present that the highest probability of operation phase risk results from cybersecurity risk, which leads to data security and privacy risk, with a value of 40%.

For smart city users, who are mostly information technology managers, it is necessary to raise awareness of the holistic view of risks. Special risk scenarios may occur due to wrong operation, lack of security awareness, or lack of maintenance to avoid the impacts of service disturbance in the smart city.

Prioritizing risks is performed using the resulting evaluation criteria based on the grounded theory from this study to identify the impacts of risks on a smart city project regarding service continuity, efficiency, resource productivity, revenue generation, and reputation. The evaluation criteria provide weights for each, in addition to weights of risks during smart city project phases. The research offers suggestions for theory and practice. It is a main study that aims to fill the research gap of the limited number of comprehensive risk assessment frameworks for smart cities. Second, the proposed framework identified major incidents causing risk, with quantification of probabilities' values and their impacts. Finally, unlike methods that consider incidents or risks in an isolated manner, the framework suggested combinations of incidents causing risks and interrelated risks through scenarios that will provide decision-makers with a holistic view.

The proposed framework can be implemented with the applicable incidents for each type of risk. The decision-makers can use MS Excel tools to analyze the data. The method can be used by smart city designers, planners, implementers, operators, and decision-makers. The framework includes analytical methods which are evidenced as applicable in various project phases. Therefore, these methods can be automated to provide decision support for smart city decision-makers.

The limitation that could be counted is the number of experts and decision-makers who could evaluate the framework's output since the sample contains experts from the region and from international projects. Although the number is consistent with the literature, more experts could be used in the evaluation.

4.7 Chapter Summary

This chapter provided the results for each phase of the suggested framework. Figure 3.1. Phase 1 results provided the incidents causing risks and their ranks, and then risks were defined using the Gioia method. The outcome of this phase provided the answer to research question 1, which concerns the risk types applicable to a smart city project. The results identified eleven main risks: five are technology-related, and six are related to organizational, social, and financial factors.

Then, the ranks of incidents resulting from Phase 1 of the framework in Figure 3.1 are used to calculate the combined basic probability assignment. In real life, incidents causing risks are combined to get probability values since incidents causing risks do not occur in solos. Interrelations are identified, providing an answer to the second research question.

A graphical presentation of the relations is reached based on interviews with experts and common incidents between different risks. That led to the outcome of Phase 2 of the suggested framework in Figure 3.1, the graphical presentation of the risk scenarios. Calculating the probability of risk scenarios requires using Bayes' theory to calculate the probability of risk occurring due to combined incidents. This step represents the hybrid usage of Dempster -Shafer theory and Bayes Theory in estimating risk probability and creating risk assessment tool used in the framework.

Then, Bayesian joint probability is used to calculate the risk scenario probability. That will be evaluated using the AHP multicriteria decision-making technique. Achieving the outcome of Phase 3 of the framework Figure 3.1.

These results address the research questions of what to consider when designing a smart city risk assessment framework and how it can be implemented.

CHAPTER 5: CONCLUSIONS, CONTRIBUTIONS, AND FUTURE RESEARCH

The thesis proposed a holistic framework that can be used to assess risks in smart city projects. The framework is considered holistic since it studies technical and non-technical risks a smart city project faces during the design, planning, implementation, and operation phases. The understanding of the probabilities of these risks to occur and the interrelations between them, through the resulting risk scenarios, are used to support the decision-makers in having a better overview of the joint probabilities of risks to occur. The impacts on smart city sustainability are defined. Evaluation criteria are provided so management can build their decision based on calculations and mathematical values.

Therefore, the contribution of the thesis is on the development of a framework and the evidence that the tools are used for calculating the combined basic probability assignment (Dempster-Shafer theory), joint probability –(Bayesian Theory), and Analytical Hierarchy process as multicriteria decision-making technique, to be applied and used for risk assessment of smart city project.

Applicable risk types to smart city projects are technical and non-technical risks accompanying technology adoption, integration, and governance and must be considered to enhance smart city outcomes. Technical risks, including cybersecurity, technical data and application risk, network infrastructure risks, data security, and privacy and integration risks, are often emphasized to coexist with non-technical risks such as social, economic, governance, legal, and strategic risks. Addressing non-technical risks such as strategic risks, stakeholder engagement risks, financial risks, resource and resource management risks, and legal risks can significantly enhance smart city outcomes during design, planning, implementation, and operation. A holistic smart city risk assessment framework that balances technical and non-technical aspects is essential for successful smart city endeavors.

There are interrelations among different types of risks. These interrelations emerge from expert interviews and correlation tests on the data. Technical risks often stem from shared incidents. For example, cybersecurity, technical data, and application risks may arise due to a lack of integration and interoperability between systems or security awareness. Cybersecurity and technical data and application risks exhibit correlations, and common incidents include cyber-attacks and security awareness. Smart City Experts believe that technical risks intertwine with non-technical risks.

For instance, laws, regulations, and standards risk relate to integration risk. A lack of awareness about regulations and standards can trigger integration risks. Thus, understanding these interrelations is essential for effective risk management and informed decision-making in complex systems.

When performing smart city risk assessment, risks interrelations. Main risk scenarios for different project phases of design, planning, implementation, and operation should be specified. Risk incident probabilities must be considered when calculating joint probabilities of risk scenarios to provide a comprehensive understanding. Also, recognizing the impacts of risks on smart city projects and overall city sustainability is essential, including the impacts on service continuity, efficiency, resource productivity, reputation, and revenue generation. Evaluation of risks and impacts will support decision-makers to take appropriate mitigation measures.

The suggested framework aims to identify, analyze, and prioritize risks across different phases of a smart city project. During the design phase, attention should be paid to strategic, stakeholder engagement, laws and regulations, business continuity, and financial risks. In the planning phase, decision-makers find financial risk in addition to the design phase risks. Resource and resource management risks also require attention.

During the implementation phase, it is mandatory to protect smart city systems from cyber threats; implementers must address vulnerabilities, secure networks, and safeguard data. Reliable and robust network infrastructure ensures seamless communication between devices and services.

Furthermore, integrating various components (applications, hardware, sensors) requires careful planning to avoid compatibility issues. During the operation phase, in addition to the attention to technology-related risks, regular communication among stakeholders expedites implementation and operation. Reference to strategic plans and ensure alignment with project goals. In addition, understanding local legislation is a must to avoid delays, additional costs, and reputational impacts.

During the operation phase, the team must be aware of risks communicated by planning and implementation teams. This is required to build effective risk management and ensure service continuity and productivity. With the application of the holistic framework, smart city projects can navigate challenges, enhance efficiency, and achieve their intended impact.

Accordingly, the objective of the thesis to propose a generic risk analysis framework and evaluate its applicability in smart city design and operation is achieved.

The literature is reviewed to identify the current research and available smart city risk assessment framework to build a comprehensive smart city risk assessment framework. The available frameworks are evaluated against their inclusive point of view of different types of risks related to various smart city dimensions.

5.1Contributions

The thesis contributes by proposing a comprehensive risk assessment framework and analytical models to assess the impact of technical risk and non-technical risks associated with different dimensions in any phase of a smart city project. The framework is developed by using management research (grounded theory) and quantitative research (Dempster-Shafer theory and Bayesian Network theory).

5.2 Limitations

1. Probabilities to be used in the Dempster-Shafer theory are defined based on the outcomes obtained from the interviews. Such probabilities might be changed when the decision-making environment changes. Therefore, although the framework and tools used in the thesis are robust, the implication of belief and recommendation is valid for the situation governed during the study conducted for this thesis.
2. The thesis uses Dempster-Shafer's theory as a risk assessment method as it can replicate the belief of a particular expert based on her/his in-depth experience in one or many phases of the smart city project. The theory was used as it was cited as an applicable method to obtain experts' beliefs on risk occurrence (Sentz & Ferson, 2002). The methods like Mote Carlo simulation could also have been used to develop the relation between the risks. However, the focus here was to have directional aspects related to risks. Therefore, the Bayesian method is considered more useful.
3. The calculation of risk probability to occur depends on the probabilities of incidents causing risk. Some risks occurring in a phase can impact other phases

of the project. Also, some risks in the later phase may be noticed due to the issues in the previous phases. However, this kind of cascaded risk in different phases is not considered in this thesis.

5.3 Future Research

1. This research considered technical and non-technical risks affecting the smart city project life cycle based on the inputs from the interviewers and the literature. External factors like the impact of climate change, political processes, or supply chain factors can also impact smart city projects. Fernández & Peek (2020) also mention that smart cities need to adapt to climate change situations. Miller (2020) mentions the impact of the political situation on smart cities. Therefore, future research can be conducted to extend the framework and assess the combined impact of external factors on the smart city project lifecycle.
2. Smart city systems produce big data, which can provide valuable insight into risk triggers. Global organizations use big data analytics to assess risks within their organizations (El Khatib et al., 2023). Therefore, although the analysis requires multidisciplinary expertise, utilizing big data can help understand the association among the risks, cause and impact relations, and potential risk triggers or patterns. Therefore, integrating the proposed framework with big data analytics for risk assessment and developing cause-and-effect relations can be considered for future research. Developing algorithms and small changes in the framework could be the main focus of such research.
3. Smart city projects become complex as they require the collaboration of different departments to manage risks (Thamhain, 2008).Therefore, the proposed framework can be extended to examine the risks that can be carried

forward from one phase to another and develop analytical models to do so. This may require analysis to be carried out in stages and relating the impact in the later stages to the risks or issues that may have happened in the earlier stages. This type of analysis will make the analytical model NP-hard. Therefore, the utilization or development of heuristics will be required to assist in decision-making.

REFERENCES

Abie, H., & Balasingham, I. (2013). *Risk-Based Adaptive Security for Smart IoT in eHealth*. *SeTTIT*, 269–275. https://doi.org/10.4108/icst.bodynets.2012.250235

Adikari, S., McDonald, C., & Campbell, J. (2009). Little design up-front: A design science approach to integrating usability into agile requirements engineering. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5610 LNCS*(PART 1), 549–558. https://doi.org/10.1007/978-3-642-02574-7_62

Ahad, M. A., Paiva, S., Tripathi, G., & Feroz, N. (2020). Enabling technologies and sustainable smart cities. *Sustainable Cities and Society*, *61*(March), 102301. https://doi.org/10.1016/j.scs.2020.102301

Akande, A., Cabral, P., & Casteleyn, S. (2020). Understanding the sharing economy and its implication on sustainability in smart cities. *Journal of Cleaner Production*, *277*, 124077. https://doi.org/10.1016/j.jclepro.2020.124077

Alawad, H., An, M., & Kaewunruen, S. (2020). Utilizing an adaptive neuro-fuzzy inference system (ANFIS) for overcrowding level risk assessment in railway stations. *Applied Sciences (Switzerland)*, *10*(15). https://doi.org/10.3390/app10155156

Allam, Z., & Dhunny, Z. A. (2019). On big data, artificial intelligence and smart cities. *Cities*, *89*(January), 80–91. https://doi.org/10.1016/j.cities.2019.01.032

Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020). Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*, *54*(February 2019), 101728. https://doi.org/10.1016/j.scs.2019.101728

Apostol, D., Bălăceanu, C., & Constantinescu, E. M. (2015). Smart – Economy Concept – Facts And Perspectives. *HOLISTICA Journal of Business and Public*

Administration, *6*(3), 67–77.

Apostolopoulos, V., Giourka, P., Martinopoulos, G., Angelakoglou, K., Kourtzanidis, K., & Nikolopoulos, N. (2022). Smart readiness indicator evaluation and cost estimation of smart retrofitting scenarios - A comparative case-study in European residential buildings. *Sustainable Cities and Society*, *82*(May), 103921. https://doi.org/10.1016/j.scs.2022.103921

Appio, F. P., Lima, M., & Paroutis, S. (2019). Understanding Smart Cities: Innovation ecosystems, technological advancements, and societal challenges. *Technological Forecasting and Social Change*, *142*(December 2018), 1–14. https://doi.org/10.1016/j.techfore.2018.12.018

Arroub, A., Zahi, B., Sabir, E., & Sadik, M. (2016). A literature review on Smart Cities: Paradigms, opportunities and open problems. *Proceedings - 2016 International Conference on Wireless Networks and Mobile Communications, WINCOM 2016: Green Communications and Networking*, 180–186. https://doi.org/10.1109/WINCOM.2016.7777211

Atitallah, S. Ben, Driss, M., Boulila, W., & Ghézala, H. Ben. (2020). Leveraging Deep Learning and IoT big data analytics to support the smart cities development: Review and future directions. *Computer Science Review*, *38*, 100303. https://doi.org/10.1016/j.cosrev.2020.100303

Awasthi, A., & Chauhan, S. S. (2011). Using AHP and Dempster-Shafer theory for evaluating sustainable transport solutions. *Environmental Modelling and Software*, *26*(6), 787–796. https://doi.org/10.1016/j.envsoft.2010.11.010

Ayres, D., Schmutte, J., & Stanfield, J. (2017). Expect the unexpected: Risk assessment using Monte Carlo simulations. *Journal of Accountacy*. https://www.journalofaccountancy.com/issues/2017/nov/risk-assessment-using-monte-carlo-simulations.html

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N., & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, 3–13. https://doi.org/10.1016/j.diin.2017.06.015

Beenish, H., Javid, T., Fahad, M., Siddiqui, A. A., Ahmed, G., & Syed, H. J. (2023). A Novel Markov Model-Based Traffic Density Estimation Technique for Intelligent Transportation System. *Sensors*, *23*(2), 1–24. https://doi.org/10.3390/s23020768

Belanche-gracia, D., Casaló-ariño, L. V, & Pérez-rueda, A. (2015). Determinants of multi-service smartcard success for smart cities development : A study based on citizens ' privacy and security perceptions. *Government Information Quarterly*, *32*(2), 154–163. https://doi.org/10.1016/j.giq.2014.12.004

Ben Yahia, N., Eljaoued, W., Bellamine Ben Saoud, N., & Colomo-Palacios, R. (2019). Towards sustainable collaborative networks for smart cities co-governance. *International Journal of Information Management*, *February*, 102037. https://doi.org/10.1016/j.ijinfomgt.2019.11.005

Bibri, S. E., & Krogstie, J. (2017). Smart sustainable cities of the future: An extensive interdisciplinary literature review. *Sustainable Cities and Society*, *31*, 183–212. https://doi.org/10.1016/j.scs.2017.02.016

Biemel, W., & Spiegelberg, H. (2024). phenomenology. In *Encyclopedia Britannica*. https://www.britannica.com/topic/phenomenology

Botello, J. V., Mesa, A. P., Rodríguez, F. A., Díaz-López, D., Nespoli, P., & Mármol, F. G. (2020). BlockSIEM: Protecting smart city services through a blockchain-based and distributed SIEM. *Sensors (Switzerland)*, *20*(16), 1–22. https://doi.org/10.3390/s20164636

Bouramdane, A.-A. (2024). Enhancing disaster management in smart cities through MCDM-AHP analysis amid 21st century challenges. *Information System and Smart City*, *3*(1), 1–19. https://doi.org/10.59400/issc.v3i1.189

Bouzguenda, I., Alalouch, C., & Fava, N. (2019). Towards smart sustainable cities: A review of the role digital citizen participation could play in advancing social sustainability. *Sustainable Cities and Society*, *50*(November 2018), 101627. https://doi.org/10.1016/j.scs.2019.101627

Boyd, M. A. (1998). *An Introduction to Markov Modeling: Concepts and Uses*. 26. https://ntrs.nasa.gov/search.jsp?R=20020050518%0Ahttps://ntrs.nasa.gov/search.jsp?R=20020050518%0Ahttps://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20020050518.pdf

Brooke, J. (2020). SUS: A “Quick and Dirty” Usability Scale. *Usability Evaluation In Industry*, *January 1996*, 207–212. https://doi.org/10.1201/9781498710411-35

Bujang, M. A., Omar, E. D., & Baharum, N. A. (2018). *Original Article A Review on Sample Size Determination for Cronbach ’ s Alpha Test : A Simple Guide for Researchers*. *25*(6), 85–99.

Calciolari, S., González Ortiz, L., Goodwin, N., & Stein, V. (2022). Validation of a conceptual framework aimed to standardize and compare care integration initiatives: the project INTEGRATE framework. *Journal of Interprofessional Care*, *36*(1), 152–160. https://doi.org/10.1080/13561820.2020.1864307

Canco, I., Kruja, D., & Iancu, T. (2021). Ahp, a reliable method for quality decision making: A case study in business. *Sustainability (Switzerland)*, *13*(24), 1–14. https://doi.org/10.3390/su132413932

Carter, D. (2013). Urban Regeneration, Digital Development Strategies and the Knowledge Economy: Manchester Case Study. *Journal of the Knowledge*

Economy, *4*(2), 169–189. https://doi.org/10.1007/s13132-012-0086-7

Caviglione, L., & Coccoli, M. (2020). A holistic model for security of learning applications in smart cities. *Journal of E-Learning and Knowledge Society*, *16*(1), 1–10. https://doi.org/10.20368/1971-8829/1135031

Certa, A., Hopps, F., Inghilleri, R., & La Fata, C. M. (2017). A Dempster-Shafer Theory-based approach to the Failure Mode, Effects and Criticality Analysis (FMECA) under epistemic uncertainty: application to the propulsion system of a fishing vessel. *Reliability Engineering and System Safety*, *159*(October 2016), 69–79. https://doi.org/10.1016/j.ress.2016.10.018

Chang, K. H. (2015). A novel general risk assessment method using the soft TOPSIS approach. *Journal of Industrial and Production Engineering*, *32*(6), 408–421. https://doi.org/10.1080/21681015.2015.1070375

Clemen, R. T., & Reilly, T. (2004). Making hard decisions with Decision Tools Suite. *DuxburyThomson Learning*, 688.

Coelho, V. N., Oliveira, T. A., Tavares, W., & Coelho, I. M. (2021). Smart Accounts for Decentralized Governance on Smart Cities. *Smart Cities*, *4*(2), 881–893. https://doi.org/10.3390/smartcities4020045

Čolić, N., Manić, B., Niković, A., & Brankov, B. (2020). Grasping the framework for the urban governance of smart cities in Serbia. The case of interreg SMF project clever. *Spatium*, *4*(43), 26–34. https://doi.org/10.2298/SPAT2043026C

Corbin, J., & Strauss, A. (1990). *Grounded_Theory(근거이론).Pdf*.

D'Amico, G., L'Abbate, P., Liao, W., Yigitcanlar, T., & Ioppolo, G. (2020). Understanding Sensor Cities : Insights from. *Sensors*.

Danisi, C., Dustin, M., Ferreira, N., & Held, N. (2021). The Decision-Making

Procedure. *IMISCOE Research Series*, *27*(4), 179–258. https://doi.org/10.1007/978-3-030-69441-8_6

Delavar, M. R., & Sadrykia, M. (2020). Assessment of enhanced dempster-shafer theory for uncertainty modeling in a GIS-based seismic vulnerability assessment model, case study - Tabriz city. *IEEE Transactions on Engineering Management*, *10*(4), 917–929. https://doi.org/10.1108/YC-01-2019-0940

Demircan, B. G., & Yetilmezsoy, K. (2023). A Hybrid Fuzzy AHP-TOPSIS Approach for Implementation of Smart Sustainable Waste Management Strategies. *Sustainability (Switzerland)*, *15*(8). https://doi.org/10.3390/su15086526

Deveci, M., Pekaslan, D., & Canıtez, F. (2020). The assessment of smart city projects using zSlice type-2 fuzzy sets based Interval Agreement Method. *Sustainable Cities and Society*, *53*(August 2019). https://doi.org/10.1016/j.scs.2019.101889

Domingos, P., Rita, A., Terra, T., & Ignácio, S. R. (2008). FMEA as a Tool for Managing Risks in ICT Projects , based on the PMBOK. *Asian Journal of Business and Management Sciences*, *3*(12), 1–24.

Dragan, I., & Isaic-maniu, A. (2022). *An Original Solution for Completing Research through Snowball Sampling — Handicapping Method*. 729–746. https://doi.org/10.4236/aasoci.2022.1211052

Eduardo DEvidson Costa Bezerra, Ariel Soares Teles, Luciano Reis Countinho, & Francisco Jose da Silva. (2021). *Dempster_Shafer Theory for Modeling and TreatingUncertainty in IoT Applications Based on ComplexEvent Processing.pdf*. *21*(1863).

El-haddadeh, R., Weerakkody, V., Osmani, M., & Thakker, D. (2019). Examining citizens ’ perceived value of internet of things technologies in facilitating public sector services engagement. *Government Information Quarterly*, *36*(2), 310–320.

https://doi.org/10.1016/j.giq.2018.09.009

El Khatib, M., Ankit, A., Al Ameeri, I., Al Zaabi, H., Al Marqab, R., Alzoubi, H. M., & Alshurideh, M. (2023). The Role and Impact of Big Data in Organizational Risk Management. In M. Alshurideh, A. K. B. Hikmat, R. Masa'deh, A. H. M., & S. Salloum (Eds.), *The Effect of Information Technology on Business and Marketing Intelligence Systems* (pp. 2139–2153). Springer International Publishing. https://doi.org/10.1007/978-3-031-12382-5_117

Elahi, H., Wang, G., Peng, T., & Chen, J. (2019). On transparency and accountability of smart assistants in smart cities. *Applied Sciences (Switzerland), 9*(24). https://doi.org/10.3390/app9245344

Elçi, A., & Çubukçuo, B. (2014). *A Narrative Research Approach : The Experiences*. 36–42.

Escorcia Guzman, J. H., Zuluaga-Ortiz, R. A., Barrios-Miranda, D. A., & Delahoz-Dominguez, E. J. (2021). Information and Communication Technologies (ICT) in the processes of distribution and use of knowledge in Higher Education Institutions (HEIs). *Procedia Computer Science*, *198*(2021), 644–649. https://doi.org/10.1016/j.procs.2021.12.300

Fernandez-Anez, V., Velazquez, G., Perez-Prada, F., & Monzón, A. (2018). Smart City Projects Assessment Matrix: Connecting Challenges and Actions in the Mediterranean Region. *Journal of Urban Technology*, *0*(0), 1–25. https://doi.org/10.1080/10630732.2018.1498706

Fernández, C. G., & Peek, D. (2020). Smart and sustainable? Positioning adaptation to climate change in the european smart city. *Smart Cities*, *3*(2), 511–526. https://doi.org/10.3390/smartcities3020027

Furuncu, E., & Sogukpinar, I. (2015). Scalable risk assessment method for cloud computing using game theory (CCRAM). *Computer Standards and Interfaces*, *38*, 44–50. https://doi.org/10.1016/j.csi.2014.08.007

Gan, D., Yang, B., & Tang, Y. (2020). An extended base belief function in dempster–shafer evidence theory and its application in conflict data fusion. *Mathematics*, *8*(12), 1–19. https://doi.org/10.3390/math8122137

Gavurova, B., Kelemen, M., & Polishchuk, V. (2022). Expert model of risk assessment for the selected components of smart city concept: From safe time to pandemics as COVID-19. *Socio-Economic Planning Sciences*, *82*(PB), 101253. https://doi.org/10.1016/j.seps.2022.101253

Ghosh, N., Paul, R., Maity, S., Maity, K., & Saha, S. (2020). Fault Matters: Sensor data fusion for detection of faults using Dempster–Shafer theory of evidence in IoT-based applications. *Expert Systems with Applications*, *162*(July), 113887. https://doi.org/10.1016/j.eswa.2020.113887

Gioia, D. (2021). A Systematic Methodology for Doing Qualitative Research. *The Journal of Applied Behavioral Science*, *57*(1), 20–29. https://doi.org/10.1177/0021886320982715

Gioia, D. A. (2000). *Organizational Identity , Image , and Adaptive Instability Author (s): Dennis A . Gioia , Majken Schultz and Kevin G . Corley Published by : Academy of Management Stable URL : https://www.jstor.org/stable/259263 REFERENCES Linked references are availabl*. *25*(1), 63–81.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Glaser, B. G., Strauss, A. L., & Strutzel, E. (1968). The Discovery of Grounded Theory; Strategies for Qualitative Research. *Nursing Research*, *17*(4).

https://journals.lww.com/nursingresearchonline/fulltext/1968/07000/the_discovery_of_grounded_theory__strategies_for.14.aspx

Golubchikov, O., & Thornbush, M. (2020). Artificial Intelligence and Robotics in Smart City Strategies and Planned Smart Development. *Smart Cities*, *3*(4), 1133–1144. https://doi.org/10.3390/smartcities3040056

Guinhouya, K. A. (2023). Bayesian networks in project management: A scoping review. *Expert Systems with Applications*, *214*(October 2022), 119214. https://doi.org/10.1016/j.eswa.2022.119214

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

Hamilton, E. (2020). The Benefits and Risks of Policymakers' Use of Smart City Technology. *SSRN Electronic Journal*, *October*. https://doi.org/10.2139/ssrn.3191449

Helfert, M., Krempels, K. H., Klein, C., Donnellan, B., & Gusikhin, O. (2015). Smart cities, green technologies, and intelligent transport systems: 4th international conference, SMARTGREENS 2015 and 1st international conference VEHITS 2015 Lisbon, Portugal, May 20–22, 2015 revised selected papers. *Communications in Computer and Information Science, 579,* 1–11.

Hevner, A., & Chatterjee, S. (2010). *Design Science Research in Information Systems*. 9–22. https://doi.org/10.1007/978-1-4419-5653-8_2

Hussein, M., Hirst, S., Salyers, V., & Osuji, J. (2014). Using Grounded Theory as a Method of Inquiry: Advantages and Disadvantages. *The Qualitative Report*, *19*, 1–14. https://doi.org/10.46743/2160-3715/2014.1209

Hwang, C.-L., & Yoon, K. (1981). *Basic Concepts and Foundations*. 16–57. https://doi.org/10.1007/978-3-642-48318-9_2

Isaac, E. (2023). *Convenience and Purposive Sampling Techniques: Are they the Same? 11*(1), 1–7. www.seahipaj.org

Ismagilova, E., Hughes, L., Dwivedi, Y. K., & Raman, K. R. (2019). Smart cities: Advances in research—An information systems perspective. *International Journal of Information Management*, *47*(December 2018), 88–100. https://doi.org/10.1016/j.ijinfomgt.2019.01.004

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-020-10044-1

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Information Systems Frontiers, 24*(2), 393–414. https://doi.org/10.1007/s10796-020-10044-1

Jayarathna, C. P., Agdas, D., & Dawes, L. (2022). Exploring sustainable logistics practices toward a circular economy: A value creation perspective. *Business Strategy and the Environment*, *January*, 1–17. https://doi.org/10.1002/bse.3170

Joseph, D., Kok-Yee, N., Christine, K., & Soon Ang. (2007). Turnover of Information Technology Professionals: A Narrative Review, Meta-Analytic Structural Equation Modeling, and Model Development. *MIS Quarterly, 31*(3), 547–577.

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *Eurasip Journal on Information Security*, *2020*(1).

https://doi.org/10.1186/s13635-020-00111-0

Kayacan, E., & Khanesar, M. A. (2016). Fundamentals of Type-1 Fuzzy Logic Theory. *Fuzzy Neural Networks for Real Time Control Applications*, 13–24. https://doi.org/10.1016/b978-0-12-802687-8.00002-5

Kirimtat, A., Krejcar, O., Kertesz, A., & Tasgetiren, M. F. (2020). Future Trends and Current State of Smart City Concepts: A Survey. *IEEE Access*, *8*, 86448–86467. https://doi.org/10.1109/ACCESS.2020.2992441

Kummitha, R. K. R., & Crutzen, N. (2019). Smart cities and the citizen-driven internet of things: A qualitative inquiry into an emerging smart city. *Technological Forecasting and Social Change*, *140*(December 2018), 44–53. https://doi.org/10.1016/j.techfore.2018.12.001

Laato, S., Mäntymäki, M., Islam, A. K. M. N., Hyrynsalmi, S., & Birkstedt, T. (2022). Trends and Trajectories in the Software Industry: implications for the future of work. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-022-10267-4

Leach, T. (2014). *Methodologies: Phenomenology*.

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, *12*(9), 157. https://doi.org/10.3390/fi12090157

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Lee, J., & Kim, J. (2007). Grounded theory analysis of e-government initiatives: Exploring perceptions of government authorities. *Government Information Quarterly*, *24*(1), 135–147. https://doi.org/10.1016/j.giq.2006.05.001

Lewis, J. R., & Sauro, J. (2018). Item Benchmarks for the System Usability Scale. *Journal of Usability Studies*, *13*(January), 158–167.

Lichy, J., McLeay, F., Burdfield, C., & Matthias, O. (2022). Understanding pre-teen consumers social media engagement. *International Journal of Consumer Studies, March*, 1–14. https://doi.org/10.1111/ijcs.12821

Löfgren, K., & Webster, C. W. R. (2020). The value of Big Data in government: The case of 'smart cities.' *Big Data and Society, 7*(1). https://doi.org/10.1177/2053951720912775

López, M. (2022). The effect of sampling mode on response rate and bias in elite surveys. *Quality and Quantity, 57*(2), 1303–1319. https://doi.org/10.1007/s11135-022-01406-9

Lyu, H. M., Yin, Z. Y., Zhou, A., & Shen, S. L. (2023). MCDM-based flood risk assessment of metro systems in smart city development: A review. *Environmental Impact Assessment Review*, *101*(July 2022), 107154. https://doi.org/10.1016/j.eiar.2023.107154

Malhotra, H., Bhargava, R., & Dave, M. (2017). Implementation of E-Governance projects: Development, Threats & Targets. *JIMS8I � International Journal of Information Communication and Computing Technology, 5*(2), 292. https://doi.org/10.5958/2347-7202.2017.00009.3

Mateo, J. R. S. C. (2012). Multi-Criteria Analysis in the Renewable Energy Industry. *Green Energy and Technology*, *83*, 0–3. https://doi.org/10.1007/978-1-4471-2346-0

Meadowcroft, J., Stephens, J. C., Wilson, E. J., & Rowlands, I. H. (2018). Social dimensions of smart grid: Regional analysis in Canada and the United States. Introduction to special issue of Renewable and Sustainable Energy Reviews.

Renewable and Sustainable Energy Reviews, *82*(June 2017), 1909–1912. https://doi.org/10.1016/j.rser.2017.06.106

Measuring well-being and progress. (n.d.).

Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., & Guizani, S. (2017). Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. *IEEE Communications Magazine*, *55*(9), 16–24. https://doi.org/10.1109/MCOM.2017.1600514

Mikes, A. (2012). *Managing Risks: A New Framework*. *June*. https://ora.ox.ac.uk/objects/uuid:b7f8eecb-9d51-4301-9999-01385bdd0284/download_file?safe_filename=Kaplan_and_Mikes_Managing_risks.pdf&type_of_work=Journal+article

Miller, T. R. (2020). Imaginaries of Sustainability: The Techno-Politics of Smart Cities. *Science as Culture*, *29*(3), 365–387. https://doi.org/10.1080/09505431.2019.1705273

Murray, M. (2017). *The calculation of percentages and means from data in a Blackboard Enterprise Survey*. *February*, 1–5. http://community.dur.ac.uk/lt.team/wp-content/uploads/2017/01/Enterprise_Survey.pdf

Nilssen, M. (2019). To the smart city and beyond? Developing a typology of smart urban innovation. *Technological Forecasting and Social Change*, *142*(July 2018), 98–104. https://doi.org/10.1016/j.techfore.2018.07.060

Nitoslawski, S. A., Galle, N. J., van den Bosc, C. K., & Steenberg, J. W. N. (2019). Smarter ecosystems for smarter cities? A review of trends, technologies, and turning points for smart urban forestry. *Sustainable Cities and Society*, *51*(August), 101770. https://doi.org/10.1016/j.scs.2019.101770

Nižetić, S., Šolić, P., López-de-Ipiña González-de-Artaza, D., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*. https://doi.org/10.1016/j.jclepro.2020.122877

Ntinda, K. (2017). Handbook of Research Methods in Health Social Sciences. *Handbook of Research Methods in Health Social Sciences*, *July*, 171–183. https://doi.org/10.1007/978-981-10-2779-6

O'Dwyer, E., Pan, I., Acha, S., & Shah, N. (2019). Smart energy systems for sustainable smart cities: Current developments, trends and future directions. *Applied Energy*, *237*(November 2018), 581–597. https://doi.org/10.1016/j.apenergy.2019.01.024

Orejon-Sanchez, R. D., Crespo-Garcia, D., Andres-Diaz, J. R., & Gago-Calderon, A. (2022). Smart cities' development in Spain: A comparison of technical and social indicators with reference to European cities. *Sustainable Cities and Society*, *81*(February 2021), 103828. https://doi.org/10.1016/j.scs.2022.103828

Paiva, S., Ahad, M. A., Tripathi, G., Feroz, N., & Casalino, G. (2021). Enabling technologies for urban smart mobility: Recent trends, opportunities and challenges. *Sensors*, *21*(6), 1–45. https://doi.org/10.3390/s21062143

Patrão, C., Moura, P., & Almeida, A. T. de. (2020). Review of Smart City Assessment Tools. *Smart Cities*, *3*(4), 1117–1132. https://doi.org/10.3390/smartcities3040055

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). *Sensing as a service model for smart cities supported*. *September 2013*, 81–93. https://doi.org/10.1002/ett

Pokharel, S. (2023). Introducing BLOC-ICE for Exploring System Concept. *International Journal of Business and Systems Research*, *17*(4), 442–461. https://doi.org/10.1504/ijbsr.2022.10039739

Porru, S., Misso, F. E., Pani, F. E., & Repetto, C. (2020). Smart mobility and public transport: Opportunities and challenges in rural and urban areas. *Journal of Traffic and Transportation Engineering (English Edition)*, *7*(1), 88–97. https://doi.org/10.1016/j.jtte.2019.10.002

Prevelianaki, K., & Sherratt, F. (2023). *Big Data Analysis on Complex Network — with the example of smart city Big Data Analysis on Complex Network — with the example of smart city*. https://doi.org/10.1088/1742-6596/2425/1/012030

Priyanka, E. B., & Thangavel, S. (2020). Influence of internet of things (IoT) in association of data mining towards the development smart cities-A review analysis. *Journal of Engineering Science and Technology Review*, *13*(4), 1–21. https://doi.org/10.25103/jestr.134.01

Radanliev, P., De Roure, D. C., Nurse, J. R. C., Montalvo, R. M., Burnap, P., Roure, D. C. De, Nurse, J. R. C., Montalvo, R. M., Stacy Cannady, Burnap, P., Eirini Anthi, Ani, U., Maddox, L., Santos, O., & Montalvo, R. M. (2019). Design principles for cyber risk impact assessment from Internet of Things (IoT). *University of Oxford Combined Working Papers and Project Reports Prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre*, *March*. https://doi.org/10.13140/RG.2.2.33014.86083

Radonjic-Simic, M., & Pfisterer, D. (2019). Beyond platform economy: A comprehensive model for decentralized and self-organizing markets on internet-scale. *Computers*, *8*(4), 1–44. https://doi.org/10.3390/computers8040090

Radu, L.-D. (2020). Disruptive Technologies in Smart Cities: A Survey on Current Trends and Challenges. *Smart Cities*, *3*(3), 1022–1038. https://doi.org/10.3390/smartcities3030051

Roghanian, E., & Mojibian, F. (2015). Using fuzzy FMEA and fuzzy logic in project risk management. *Iranian Journal of Management Studies (IJMS)*, *8*(3), 373–395.

Romero, M., Guédria, W., Panetto, H., & Barafort, B. (2020). Towards a Characterisation of Smart Systems: A Systematic Literature Review. *Computers in Industry*, *120*. https://doi.org/10.1016/j.compind.2020.103224

Russo, Osaria;Camanho, R. (2015). Criteria in AHP: a Systematic Review of Literature. *Information Technology and Quantitative Management (ITQM 2015)*.

Saaty, R. W. (1987). The analytic hierarchy process-what it is and how it is used. *Mathematical Modelling*, *9*(3–5), 161–176. https://doi.org/10.1016/0270-0255(87)90473-8

Saaty, T. L. (2013). The modern science of multicriteria decision making and its practical applications: The AHP/ANP approach. *Operations Research*, *61*(5), 1101–1118. https://doi.org/10.1287/opre.2013.1197

Sadik, S., Ahmed, M., Sikos, L. F., & Najmul Islam, A. K. M. (2020). Toward a sustainable cybersecurity ecosystem. *Computers*, *9*(3), 1–17. https://doi.org/10.3390/computers9030074

Schiavone, F., Risitano, M., Appio, P., & Mora, L. (2020). *The strategic , organizational , and entrepreneurial evolution of smart cities*. 1155–1165.

Schweizer, K., Ren, X., & Wang, T. (2015). A comparison of confirmatory factor analysis of binary data on the basis of tetrachoric correlations and of probability-based covariances: A simulation study. In *Springer Proceedings in Mathematics and Statistics* (Vol. 89). https://doi.org/10.1007/978-3-319-07503-7_17

Secinaro, S., Brescia, V., Calandra, D., & Biancone, P. (2021). Towards a hybrid model for the management of smart city initiatives. *Cities*, *116*(February), 103278. https://doi.org/10.1016/j.cities.2021.103278

Sengan, S., Subramaniyaswamy, V., Nair, S. K., Indragandhi, V., Manikandan, J., &

Ravi, L. (2020). Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. *Future Generation Computer Systems*, *112*, 724–737. https://doi.org/10.1016/j.future.2020.06.028

Sentz, K., & Ferson, S. (2002). Combination of Evidence in Dempster- Shafer Theory. *Contract*, *April*, 96. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.122.7929&amp;rep=rep1&amp;type=pdf

Sharma, M., Joshi, S., Kannan, D., Govindan, K., Singh, R., & Purohit, H. C. (2020). Internet of Things (IoT) adoption barriers of smart cities' waste management: An Indian context. *Journal of Cleaner Production*, *270*, 122047. https://doi.org/10.1016/j.jclepro.2020.122047

Shayan, S., Kim, K. P., Ma, T., & Nguyen, T. H. D. (2020). The first two decades of smart city research from a risk perspective. *Sustainability (Switzerland)*, *12*(21), 1–20. https://doi.org/10.3390/su12219280

Shishkina, E. D. (2015). Bayesian networks as probabilistic graphical model for economical risk assessment. *Proceedings of International Conference on Soft Computing and Measurements, SCM 2015*, 24–26. https://doi.org/10.1109/SCM.2015.7190400

Shubik, M. (1958). Studies and Theories of Decision Making. *Administrative Science Quarterly*, *3*(2), 289–306.

Silva, B. N., Khan, M., & Han, K. (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities and Society*, *38*(August 2017), 697–713. https://doi.org/10.1016/j.scs.2018.01.053

Singh, P., & Helfert, M. (2019). Smart cities and associated risks: Technical v/s non-technical perspective. *CHIRA 2019 - Proceedings of the 3rd International Conference on Computer-Human Interaction Research and Applications*, *May*, 221–228. https://doi.org/10.5220/0008494402210228

Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., & Ra, I. H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and Society*, *63*(April). https://doi.org/10.1016/j.scs.2020.102364

Soltani, A., Sadiq, R., & Hewage, K. (2016). Selecting sustainable waste-to-energy technologies for municipal solid waste treatment: A game theory approach for group decision-making. *Journal of Cleaner Production*, *113*, 388–399. https://doi.org/10.1016/j.jclepro.2015.12.041

Song, X., Jiang, W., Liu, X., Lu, H., Tian, Z., & Du, X. (2020). A Survey of Game Theory as Applied to Social Networks. *Tsinghua Science and Technology*, *25*(6), 734–742. https://doi.org/10.26599/TST.2020.9010005

Sovacool, B. K., & Furszyfer Del Rio, D. D. (2020). Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and Sustainable Energy Reviews*, *120*(May 2019), 109663. https://doi.org/10.1016/j.rser.2019.109663

Spehr, J. (2015). Probabilistic graphical models. In *Studies in Systems, Decision and Control* (Vol. 11). https://doi.org/10.1007/978-3-319-11325-8_2

Srivastava, R. P., Mock, T. J., & Gao, L. (2011). The Dempster-Shafer Theory: An Introduction and Fraud Risk Assessment Illustration. *Australian Accounting Review*, *21*(3), 282–291. https://doi.org/10.1111/j.1835-2561.2011.00135.x

Staffans, A., & Horelli, L. (2014). *Expanded urban planning as a vehicle for understanding and shaping smart , Expanded Urban Planning as a Vehicle for*

Understanding and Shaping Smart , Liveable Cities. *November*.

Stephenson, T. (2000). Main Bayesian Network Auxiliary Article. *Idiap Research Report*, 31. http://ftp.idiap.ch/pub/reports/2000/rr00-03.pdf

Subriadi, A. P., & Najwa, N. F. (2020). The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment. *Heliyon*, *6*(1), e03161. https://doi.org/10.1016/j.heliyon.2020.e03161

Summers, C. (2022). Narrative theory. In *The Routledge Handbook of Translation and Methodology* (Issue March). https://doi.org/10.4324/9781315158945-19

Sun, J., Yan, J., & Zhang, K. Z. K. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, *2*(1). https://doi.org/10.1186/s40854-016-0040-y

Sun, L., Srivastava, R. P., & Mock, T. J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems*, *22*(4), 109–142. https://doi.org/10.2753/MIS0742-1222220405

Taherdoost, H., & Madanchian, M. (2023). Multi-Criteria Decision Making (MCDM) Methods and Concepts. *Encyclopedia*, *3*(1), 77–87. https://doi.org/10.3390/encyclopedia3010006

Techatassanasoontorn, A. A., & Suo, S. (2010). Exploring risks in smart city infrastructure projects: Municipal broadband initiatives. *PACIS 2010 - 14th Pacific Asia Conference on Information Systems*, 13–24.

Thamhain, H. (2008). Project Portfolio Control and Portfolio. *Project Management Journal*, *39*(April), 28–42. https://doi.org/10.1002/pmj

Tyagi, M., Kumar, P., & Kumar, D. (2014). A hybrid approach using AHP-TOPSIS for analyzing e-SCM performance. *Procedia Engineering*, *97*, 2195–2203.

https://doi.org/10.1016/j.proeng.2014.12.463

Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., & Sepasgozar, S. M. E. (2021). Risk management in sustainable smart cities governance: A TOE framework. *Technological Forecasting and Social Change*, *167*(November 2020), 120743. https://doi.org/10.1016/j.techfore.2021.120743

Ullah, I. (2018). *applied sciences Analytical Modeling for Underground Risk Assessment in Smart Cities*. https://doi.org/10.3390/app8060921

Van Aken, J. E. (2004). Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules. *Journal of Management Studies*, *41*(2), 219–246. https://doi.org/10.1111/j.1467-6486.2004.00430.x

VanScoy, A., & Evenstad, S. B. (2015). Interpretative phenomenological analysis for lis research. *Journal of Documentation*, *71*(2), 338–357. https://doi.org/10.1108/JD-09-2013-0118

Vidiasova, L., & Cronemberger, F. (2020). Discrepancies in perceptions of smart city initiatives in Saint Petersburg, Russia. *Sustainable Cities and Society*, *59*(May), 102158. https://doi.org/10.1016/j.scs.2020.102158

Vinod Kumar, T. M., & Dahiya, B. (2017). *Smart Economy in Smart Cities*. https://doi.org/10.1007/978-981-10-1610-3_1

Virag, P. (2021). Control in agile Is development projects: Looking beyond agency theory. *Procedia Computer Science*, *181*(2019), 3–14. https://doi.org/10.1016/j.procs.2021.01.093

Visvizi, A., & Troisi, O. (2022). Effective Management of the Smart City: An Outline of a Conversation. In A. Visvizi & O. Troisi (Eds.), *Managing Smart Cities: Sustainability and Resilience Through Effective Management* (pp. 1–10). Springer

International Publishing. https://doi.org/10.1007/978-3-030-93585-6_1

Vorakulpipat, C., Ko, R. K. L., Li, Q., & Meddahi, A. (2021). Security and Privacy in Smart Cities. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/9830547

Wronowski, M. L. (2018). Filling the Void: A Grounded Theory Approach to Addressing Teacher Recruitment and Retention in Urban Schools. *Education and Urban Society*, *50*(6), 548–574. https://doi.org/10.1177/0013124517713608

Wu, Y. J., & Chen, J.-C. (2021). A structured method for smart city project selection. *International Journal of Information Management*, *56*.

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Communications Surveys and Tutorials*, *21*(3), 2794–2830. https://doi.org/10.1109/COMST.2019.2899617

Yang, X., & Ma, L. (2021). AHP-Based Analysis Factors Influencing the Construction of a Smart City with Three-Dimensional Regional Color. *Journal of Sensors*, *2021*. https://doi.org/10.1155/2021/1778399

Ye, F., Chen, Y., Li, Y., & Yin, Y. (2022). Multi-criteria decision -making models for smart city ranking : Evidence from Pearl RIver Delta Region China. *Cities*, *128*.

Ye, T., Zhuang, Y., & Qiao, G. (2023). SCKPISec: A KPI-Guided Model-Based Approach to Realize Security by Design for Smart City Systems. *Sustainability (Switzerland)*, *15*(3). https://doi.org/10.3390/su15031884

Yigitcanlar, T., Desouza, K. C., Butler, L., & Roozkhosh, F. (2020). Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature. *Energies*, *13*(6). https://doi.org/10.3390/en13061473

Zakaria, H., Abu Bakar, N. A., Hassan, N. H., & Yaacob, S. (2019). IoT security risk management model for secured practice in healthcare environment. *Procedia Computer Science*, *161*, 1241–1248. https://doi.org/10.1016/j.procs.2019.11.238

Zapolskytė, S., Burinskienė, M., & Trépanier, M. (2020). Evaluation criteria of smart city mobility system using MCDM method. *Baltic Journal of Road and Bridge Engineering*, *15*(4), 196–224. https://doi.org/10.7250/bjrbe.2020-15.501

Zhang, C., Duan, X., Liu, F., Li, X., & Liu, S. (2022). Three-way Naive Bayesian collaborative filtering recommendation model for smart city. *Sustainable Cities and Society*, *76*(September 2021), 103373. https://doi.org/10.1016/j.scs.2021.103373

APPENDIX A

Interview Guide

- What are the main systems in smart city?
- What are the organizational factors that can be defined as sources of risks?
- What is the nature and type of uncertainties that affects smart city implementation and operation?

What are the main technical risks in Smart City ?

- What are the main non-technical risks in Smart City ?
- What are the main incidents causing these risks ?
- What is the likelihood of these incidents to happen (The Belief of expert).
- What are the consequences on availability of smart city systems?
- What are the consequences on accountability of Data at the smart city?
- What are the causal relations between different risks?
- What are business impacts for the identified risks?

APPENDIX B

SUS Evaluation

The Gioia Method Relations Outcome

	Strongly Disagree				Strongly Agree
1. I think that I would like to use this theory frequently.	1	2	3	4	5
2. I found the theory unnecessarily complex.	1	2	3	4	5
3. I thought the theory was easy to use.	1	2	3	4	5
4. I think that I would need the support of the researcher to be able to use this theory.	1	2	3	4	5
5. I found the various relations in this theory was well integrated.	1	2	3	4	5
6. I thought there was too much inconsistency in this theory.	1	2	3	4	5
7. I would imagine that this theory will be useful for management.	1	2	3	4	5
8. I found the theory is very cumbersome to use.	1	2	3	4	5
9. I felt confident using the theory.	1	2	3	4	5
10. I needed to learn a lot of things before I could get going. with this theory.	1	2	3	4	5

Design and Planning Phases Scenarios

	Strongly Disagree				Strongly Agree
1. I think that I would consider these scenarios during design and planning .	1	2	3	4	5
2. I found the scenarios are unnecessarily complex.	1	2	3	4	5
3. I thought the scenarios were easy to use.	1	2	3	4	5
4. I think that I would need the support of the researcher to be able to use the scenarios.	1	2	3	4	5
5. I found the various relations in These scenarios were well integrated.	1	2	3	4	5
6. I thought there was too much inconsistency in these scenarios.	1	2	3	4	5
7. I would imagine that these scenarios will be useful for the SC design and planning Team.	1	2	3	4	5
8. I found the scenarios are very cumbersome to use.	1	2	3	4	5
9. I felt confident using the scenarios.	1	2	3	4	5
10. I needed to learn a lot of things before I could get going. with these scenarios.	1	2	3	4	5

Implementation Phase Scenarios

	Strongly				Strongly
	Disagree				Agree
1. I think that I would consider these scenarios during implementation .	1	2	3	4	5
2. I found the scenarios are unnecessarily complex.	1	2	3	4	5
3. I thought the scenarios were easy to use.	1	2	3	4	5
4. I think that I would need the support of the researcher to be able to use the scenarios.	1	2	3	4	5
5. I found the various relations in These scenarios were well integrated.	1	2	3	4	5
6. I thought there was too much inconsistency in these scenarios.	1	2	3	4	5
7. I would imagine that these scenarios will be useful for the SC design and implementation Team.	1	2	3	4	5
8. I found the scenarios are very cumbersome to use.	1	2	3	4	5
9. I felt confident using the scenarios.	1	2	3	4	5
10. I needed to learn a lot of things before I could get going. with these scenarios.	1	2	3	4	5

Operation Phase Scenarios

	Strongly				Strongly
	Disagree				Agree
1. I think that I would consider these scenarios during operation .	1	2	3	4	5
2. I found the scenarios are unnecessarily complex.	1	2	3	4	5
3. I thought the scenarios were easy to use.	1	2	3	4	5
4. I think that I would need the support of the researcher to be able to use the scenarios.	1	2	3	4	5
5. I found the various relations in These scenarios were well integrated.	1	2	3	4	5
6. I thought there was too much inconsistency in these scenarios.	1	2	3	4	5
7. I would imagine that these scenarios will be useful for the SC Operations Team.	1	2	3	4	5
8. I found the scenarios are very cumbersome to use.	1	2	3	4	5
9. I felt confident using the scenarios.	1	2	3	4	5
10. I needed to learn a lot of things before I could get going. with these scenarios.	1	2	3	4	5

Evaluaition Criteria

	Strongly Disagree				Strongly Agree
1. I think that I would consider the evaluation criteria in SC Risk Management.	1	2	3	4	5
2. I found the criteria is unnecessarily complex.	1	2	3	4	5
3. I thought the criteria is easy to use.	1	2	3	4	5
4. I think that I would need the support of the researcher to be able to use the scenarios.	1	2	3	4	5
5. I found the criteria is well designed	1	2	3	4	5
6. I thought there was too much inconsistency in these scenarios .	1	2	3	4	5
7. I would imagine that the criteria will be useful for SC Management team	1	2	3	4	5
8. I found the criteria is very cumbersome to use.	1	2	3	4	5
9. I felt confident using the criteria.	1	2	3	4	5
10. I needed to learn a lot of things before I could get going. with the criteria.	1	2	3	4	5